(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 546 646**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **83 08783**

(51) Int Cl³ : G 06 R 7/00, 19/00.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 27 mai 1983.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 48 du 30 novembre 1984.

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

(71) Demandeur(s) : *Société dite : AMERICAN EXPRESS CO.* — US.

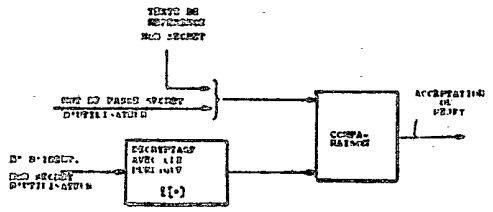
(72) Inventeur(s) : Stephen B. Weinstein.

(73) Titulaire(s) :

(74) Mandataire(s) : Blétry.

(54) Système permettant au porteur d'une carte intelligente d'exécuter des transactions au moyen d'un terminal de transactions, terminal d'initialisation de cartes intelligentes et carte intelligente portative utilisables avec un tel système.

(57) Il est décrit un système de protection pour cartes intelligentes. Il est mémorisé, dans chaque carte, un code qui est le cryptogramme de l'enchaînement d'un mot de passe secret d'utilisateur et d'un texte de référence commun. Le cryptogramme est formé par un terminal d'initialisation qui utilise une clé privée associée à une clé publique d'une paire de clés d'un système cryptographique à clé publique. Chaque terminal de transactions avec lequel une carte est utilisée décrypte le code mémorisé à l'aide de la clé publique. Une transaction n'est exécutée que si le code mémorisé donne, au décryptage, le même mot de passe d'utilisateur qui est introduit par l'intermédiaire d'un clavier, et le texte de référence commun.



FR 2 546 646 - A1

La présente invention concerne l'utilisation de cartes intelligences pour l'exécution de transactions au niveau de terminaux et, plus précisément, la prévention de l'usage frauduleux de ces cartes.

Beaucoup d'efforts ont été faits, au cours de ces dernières années, pour fournir aux usagers des cartes intelligentes, du genre "carte de crédit"; de telles cartes intelligentes comportent une mémoire et des moyens de traitement de l'information, ces derniers se présentant sous forme câblée ou, de préférence, sous la forme d'un microprocesseur à programme enregistré (bien que les recherches aient été orientées jusqu'ici vers des supports sous forme de cartes, il est bien entendu qu'une petite mémoire et un microprocesseur peuvent être logés dans d'autres supports portatifs, tels que stylos, clefs, etc.; dans sa présente acception, le terme "carte intelligente" couvre tout support qui peut être porté commodément par l'usager et qui remplit les fonctions dont il sera question ci-après). Une bonne part des recherches concernant les cartes intelligentes a été effectuée hors des Etats-Unis, et notamment en France, et un brevet antérieur qui en illustre le principe général est celui de Michel Ugon, nº 4 211 919, délivré aux Etats-Unis le 8 juillet 1980 et intitulé "Support d'information portatif, contenant un microprocesseur".

Une carte intelligente typique pourrait comporter un numéro d'identification personnel, c'est-à-dire un mot de passe secret, ainsi que le montant d'une somme en dollars (dans sa présente acception, le terme "mot de passe" désigne, soit une suite de symboles mémorisée, soit un ensemble de données numériques dérivées d'attributs physiologiques de l'utilisateur légitime de la carte, notamment de sa signature, d'un échantillon de sa voix ou de ses

empreintes digitales). L'émetteur de la carte pourrait mémoriser au départ dans la carte une valeur représentant 500 dollars, sur paiement de cette somme par l'utilisateur. Toutes les fois que la carte est utilisée dans une transaction d'achat, la valeur de la transaction est soustraite de la valeur qui reste sur la carte, la nouvelle valeur représentant le crédit disponible par l'utilisateur. Avant l'exécution de toute transaction, la carte est placée dans un terminal et il est demandé à l'utilisateur d'introduire son mot de passe (si le mot de passe est un dérivé d'attributs physiologiques, "introduire son mot de passe" doit être compris comme signifiant la fourniture d'une signature, d'un échantillon de voix, d'une empreinte digitale ou de tout autre échantillon physiologique à un dispositif analytique qui est prévu dans le terminal et qui produit le dérivé défini comme mot de passe). Si le terminal constate une concordance entre le mot de passe introduit par l'utilisateur et le mot de passe enregistré sur la carte, l'autorisation de la transaction est donnée (dans le cas d'un mot de passe dérivé d'attributs physiologiques, le terme "concordance" doit être compris comme signifiant une ressemblance acceptable, plutôt que comme une coïncidence exacte). Pour un maximum de sécurité, la comparaison des mots de passe doit se faire dans la carte elle-même : le terminal transmet à la carte le mot de passe introduit et le système logique de la carte compare le mot de passe introduit au mot de passe enregistré, pour signaler au terminal si c'est le mot de passe correct qui a été introduit. L'avantage de ne pas permettre que le mot de passe "quitte la carte" à des fins de comparaison dans le terminal est qu'il est ainsi impossible à un voleur d'identifier le mot de passe enregistré et, par conséquent, d'utiliser la carte. Si la comparaison était effectuée dans le terminal, toute personne ayant des connaissances de base en électronique pourrait avoir accès au mot de passe de la carte, une fois qu'il a été enregistré dans le terminal, et apprendre ainsi le mot de passe correct qui doit être utilisé avec la carte.

Il est bien entendu que les transactions d'achat ne sont

qu'un exemple de l'utilisation de cartes intelligentes. Comme on le sait, des cartes intelligentes peuvent être également utilisées pour avoir accès à des banques de données, pour faire des réservations d'avion, pour décrypter au niveau d'un terminal des messages en réception qui ont été transmis sous forme chiffrée, ainsi que pour de nombreuses autres applications. Un usage nouveau d'une carte intelligente est décrit dans la demande de brevet du même auteur, intitulée "Système électronique d'authentification de documents" et déposée à la même date que la présente, cette demande étant ici incluse à titre de référence. De façon générale, le terme "transaction" couvre, dans sa présente acception, toute transaction effectuée par un terminal, lorsqu'une carte intelligente d'usager y est insérée.

Un souci majeur, dans une telle utilisation de cartes intelligentes à grande échelle, est le risque de fraudes auxquelles elles peuvent se prêter. Si l'on considère qu'une carte intelligente peut permettre à son utilisateur de se procurer des centaines et même des milliers de dollars de crédit, et même, dans le cas extrême, d'obtenir de fortes sommes en argent comptant ou en travelller's chèques négociables lorsqu'un terminal de transaction est conçu pour délivrer des espèces ou des travelller's chèques, on peut comprendre aisément que les terminaux de transactions à commande par cartes ne deviendront d'usage courant que s'il existe des moyens de protection contre l'utilisation frauduleuse des cartes. La présente invention a pour but général de fournir un tel système de protection.

Il existe plusieurs genres différents de sécurité concernant les cartes intelligentes, qu'il convient de distinguer entre eux. Le premier concerne la délivrance frauduleuse de cartes authentiques. Une carte authentique est une carte produite par un fabricant autorisé pour être livrée à un émetteur de cartes, ce dernier initialisant ensuite les cartes, par exemple avec une valeur en dollars, puis les fournissant à des utilisateurs de carte. Ici, le problème est que des cartes authentiques peuvent être interceptées au cours de leur transport entre le fabricant et l'émetteur de

cartes, ou même être dérobées par des employés indélicats de l'émetteur de cartes. Des techniques ont été déjà mises au point pour la protection contre la délivrance illégitime de cartes authentiques et un système de ce genre a été incorporé dans la forme de réalisation de l'invention qui sera décrite en détail ci-après à titre d'illustration.

Le second aspect de la sécurité concernant les cartes a trait à l'utilisation d'une carte dérobée par un voleur, situation qui sera probablement banale. Comme on l'a vu, des systèmes de mots de passe secrets ont été imaginés dans l'état antérieur de la technique, pour se protéger contre l'utilisation frauduleuse d'une carte dans un cas semblable (malheureusement, aucun moyen n'a été trouvé pour venir à bout d'un criminel qui force un détenteur de carte à lui dévoiler le mot de passe. Mais les crimes violents de ce genre se produisent beaucoup moins fréquemment que les tentatives d'utilisation d'une carte dérobée. En outre, il y a exactement autant de risques à porter sur soi des espèces qu'à porter une carte intelligente lorsqu'il se produit des crimes violents de cette nature).

Le problème auquel on a été incapable d'apporter une solution jusqu'à maintenant concerne le criminel qui possède des connaissances de base approfondies en électronique. Un tel criminel pourrait effectivement fabriquer des cartes intelligentes et construire par lui-même un terminal d'initialisation, normalement réservé aux émetteurs de cartes. Il pourrait alors initialiser effectivement des cartes qui pourraient être utilisées dans les terminaux de transactions d'un émetteur de cartes légitime. Le problème est aggravé par le fait qu'un criminel doté de connaissances en électronique n'a même pas besoin de se donner autant de mal.

On peut s'attendre à ce que beaucoup de terminaux de transactions seront sans surveillance, c'est-à-dire qu'un utilisateur de carte sera en mesure d'effectuer une transaction dans un tel terminal, sans que celui-ci soit surveillé par une personne employée par l'émetteur de cartes. Beaucoup de terminaux ainsi exempts de surveillance sont déjà en place à l'heure actuelle, par exemple

ceux qui permettent au détenteur d'une carte de banque de toucher une somme en espèces pendant les heures de fermeture de la banque. Il convient de rappeler que le système de protection de base, proposé dans l'état antérieur de la technique, est l'introduction d'un mot de passe dans le terminal par l'utilisateur d'une carte et la comparaison de ce mot, dans la carte elle-même, avec le mot de passe mémorisé dans cette carte qui signale ensuite au terminal si les mots de passe concordent. La sécurité peut être complètement battue en brèche par le simple expédient consistant à insérer, dans le terminal, une carte construite spécialement. Si le terminal est agencé de telle manière que les cartes d'utilisateurs ne sont pas complètement absorbées et que le passage d'entrée n'est pas obturé, la carte peut n'être rien de plus qu'une plaquette de contacts (du format d'une carte) reliée par une série de fils à une "boîte noire" électronique que le voleur porte sur lui. Il n'est même pas nécessaire de se préoccuper de la mise en mémoire, dans la "boîte noire", d'un mot de passe que le voleur doit évidemment connaître et qu'il introduit sur le clavier du terminal. Tout ce que le voleur a à faire, c'est de délivrer au terminal, au moment opportun, un signal qui l'informe que le mot de passe introduit concorde avec le mot de passe mémorisé sur la carte. Le terminal s'attend à recevoir une réponse par "oui" ou par "non" et le falsificateur électronicien doit simplement savoir comment fournir une réponse par "oui", au moment où le terminal attend le résultat de la comparaison des mots de passe. Naturellement, le problème est particulièrement sérieux dans le cas des terminaux sans surveillance, où personne n'est là pour seulement vérifier que ce qui est placé dans le terminal "a l'air" d'une carte authentique. Dans le cas d'une carte de retrait d'espèces par exemple, il va sans dire que la "boîte noire" du falsificateur signalera au terminal que l'utilisateur de la carte dispose d'un crédit considérable.

Il a été proposé, dans l'état antérieur de la technique, un système pour parer à la fraude d'identification. Ce système, qui est commercialisé sous la marque "Identikey", sera décrit en

détail ci-après. Sa faiblesse de base consiste en ce qu'il est fondé sur une transformation de code secrète qui est mémorisée dans chaque terminal de transactions. Avec la prolifération des terminaux, il n'est pas difficile pour un falsificateur d'avoir accès à un terminal et de découvrir l'algorithme de la transformation secrète. Comme on le verra ci-après, une fois que le falsificateur a déterminé la transformation, il peut prouver son identité à la satisfaction du terminal et peut-être avoir ainsi accès à des privilèges et à des services, bien qu'il lui soit beaucoup plus difficile de présenter comme un utilisateur légitime particulier.

D'après les principes de la présente invention, il est fourni un système de protection pour cartes intelligentes qui est basé en partie sur les principes d'une nouvelle branche de la cryptographie connue sous le nom de "cryptographie à clé publique". L'un des tout premiers travaux sur la question est celui de Diffie et Hellman, "New Directions In Cryptography", IEEE Transactions On Information Theory, novembre 1976. Un autre progrès important dans ce domaine a fait l'objet d'un article publié en 1977 par Rivest, Shamir et Adleman, intitulé "On Digital Signatures And Public-Key Cryptosystems", MIT/LCS/TM-82 du Massachusetts Institute of Technology. C'est peut-être dans le numéro d'août 1979 du Scientific American, dans un article d'Hellman intitulé "The Mathematics of Public-Key Cryptography", que l'on trouvera l'exposé le plus clair de la question.

Un bref résumé de la cryptographie à clé publique est donné ci-après, les détails n'étant pas nécessaires pour que l'on puisse comprendre la présente invention. La cryptographie était essentiellement axée sur la transmission d'un message d'un point à un autre. Un système cryptographique à clé publique permet que le message soit chiffré au point A d'après une clé publique divulguée, qu'il soit transmis au point B et qu'il soit décrypté au point B d'après une clé privée secrète. La clé permettant de décrypter le message n'est connue que du destinataire au point B. Il n'y a aucun moyen efficace de déchiffrer un message sans la clé de

décryptage, alors même que l'on connaît la clé de chiffrage et le message chiffré est inutilisable par quiconque en prend connaissance illicitement. D'après un développement intéressant de l'idée de base, l'utilisation de certains systèmes de cryptographie à clé publique permet que le message soit authentifié au point A, le destinataire au point B ayant non seulement l'assurance que le message est authentique, mais étant également dans l'impossibilité de créer des messages truqués, prétendûment transmis depuis le point A, qui pourraient être tenus pour authentiques.

D'après les principes de la présente invention, l'émetteur de cartes commence par créer une paire de clés E et D de système cryptographique à clé publique. La clé secrète D est mémorisée dans un terminal d'initialisation qui est gardé dans les locaux de l'émetteur. Lorsqu'une carte est initialisée, l'utilisateur choisit un mot de passe qui est enregistré dans la carte, comme dans la technique antérieure. Mais un autre élément d'information est également mémorisé dans la carte. Cette information se compose de deux suites enchaînées qui sont chiffrées avec la clé secrète D. Une partie de la chaîne est faite du mot de passe de l'utilisateur et l'autre partie consiste en un texte de référence qui est utilisé dans tout le système. Dans le cas d'un émetteur de cartes tel que l'American Express Company, le texte de référence pourrait être tout simplement AMERICAN EXPRESS. On supposera par exemple que l'utilisateur choisit, comme mot de passe, BIGSHOT3. En utilisant la clé secrète D, le terminal d'initialisation mémorise dans la carte un cryptogramme de la suite enchaînée BIGSHOT3 AMERICAN EXPRESS.

Toutes les fois que la carte est introduite dans un terminal de transactions, le mot de passe est demandé à l'utilisateur et, de même que dans l'état antérieur de la technique, la transaction n'est autorisée que si la carte signale au terminal que le mot de passe introduit concorde avec le mot de passe mémorisé dans la carte. Comme on l'a vu, ce bas niveau de sécurité ne résiste pas à un falsificateur chevronné. Par contre, on obtient une bien plus

grande sécurité en exigeant qu'une épreuve supplémentaire en deux parties soit effectuée par le terminal et la carte, sans autre intervention de l'utilisateur. Le terminal extrait de la carte la chaîne d'information qui est le cryptogramme du mot de passe et du texte de référence enchaînés, par exemple le cryptogramme de BIGSHOT3 AMERICAN EXPRESS. Le terminal décrypte la chaîne à l'aide de la clé publique E qui est mémorisée dans le terminal. Dans le cas d'une carte valide, il en résultera la suite enchaînée BIGSHOT3 AMERICAN EXPRESS. Le terminal effectue alors deux comparaisons. La première partie de la suite enchaînée décryptée est comparée avec le mot de passe que l'utilisateur introduit sur le clavier du terminal, et la partie texte de référence de la suite décryptée est comparée avec le texte de référence AMERICAN EXPRESS qui est mémorisé dans le terminal. Ce n'est que si les deux comparaisons sont couronnées de succès que l'autorisation est donnée d'exécuter la transaction.

La protection contre les falsifications est basée sur l'impossibilité, pour le falsificateur, de créer à la fois un mot de passe et une suite chiffrée qui subissent avec succès cette épreuve ajoutée. On peut supposer qu'un falsificateur chevronné ne sera pas long à apprendre le texte de référence qui est mémorisé dans chaque terminal de transactions. Il ne sera pas long non plus à apprendre la clé publique E, par exemple en démontant un terminal de transactions. Mais sans connaître la clé secrète D, on ne voit pas comment un falsificateur pourrait trouver un code qui, introduit dans le terminal à partir de sa carte falsifiée, donnerait, au décryptage avec la clé publique mémorisée dans le terminal, une suite enchaînée se composant à la fois d'un mot de passe que ce falsificateur pourrait choisir et introduire dans le terminal et du texte prédéterminé AMERICAN EXPRESS.

Il est capital de comprendre pourquoi la suite mémorisée dans une carte doit être le cryptogramme d'un mot de passe particulier à chaque utilisateur et d'un texte de référence qui est commun à tous. Supposons qu'il soit seulement exigé de mettre en mémoire, dans une carte, le cryptogramme d'un mot de passe choisi par

l'utilisateur (en utilisant la clé privée secrète de l'émetteur de cartes). Dans un tel cas, le falsificateur, connaissant la clé publique utilisée par chaque terminal pour le décryptage, crèerait un quelconque code arbitraire pour la suite chiffrée de sa carte et utiliserait la clé publique pour la transformer en ce qu'il définirait ensuite comme son mot de passe. Il aurait simplement besoin alors d'utiliser le code arbitraire initial en tant que suite chiffrée, fournie par sa carte falsifiée au terminal, et le cryptogramme précédemment formé en tant que mot de passe qu'il introduirait sur le clavier. Il n'y a absolument aucune sécurité dans un tel système.

Supposons d'autre part qu'il soit exigé de mémoriser simplement, sur chaque carte, la suite résultant du chiffrage du texte de référence AMERICAN EXPRESS, à l'aide de la clé privée de l'émetteur de cartes. Etant donné que le même texte de référence chiffré est extrait par le terminal de transactions pour chaque carte utilisée dans le système, il n'y aurait aucune difficulté pour le falsificateur à apprendre quel code sa carte falsifiée doit fournir à un terminal quelconque pour que celui-ci le transforme par décryptage en la suite AMERICAN EXPRESS.

La sécurité de la présente invention tient précisément à la mise en mémoire, dans la carte, du cryptogramme (au moyen de la clé privée de l'émetteur) d'une combinaison d'un mot de passe particulier à l'utilisateur et d'un texte de référence commun. Il ne servira plus à rien au falsificateur de partir d'un code arbitraire. Ce code arbitraire (que la carte illicite du falsificateur fournirait au terminal) doit donner par déchiffrage deux suites, dont l'une est le texte de référence prédéterminé AMERICAN EXPRESS. Suivant les principes de cryptographie à clé publique et en supposant que les longueurs des suites sont judicieusement choisies, la probabilité est infime pour qu'un falsificateur choisisse un code arbitraire qui, déchiffré avec la clé publique, contienne une sous-suite prédéterminée. Au cas où cela arriverait, le falsificateur pourrait examiner la combinaison décryptée du mot de passe et du texte de référence et voir quel mot de passe il aurait

ensuite à introduire dans un terminal pour obtenir les deux concordances au moment où sa carte falsifiée fournit au terminal le code aléatoire qui a été essayé en premier lieu. Mais la probabilité qu'un code choisi arbitrairement donne au décryptage une suite dont une partie est un texte de référence prédéterminé, est tellement négligeable que le système atteint un niveau élevé de sécurité (une sécurité certainement suffisante pour des transactions commerciales). Le système est viable tant que le falsificateur ne peut pas déterminer la clé privée D qui est le complément de la clé publique E mémorisée dans chaque terminal de transactions. Sans la clé privée, il n'existe aucune technique, de complexité acceptable du point de vue du calcul, qui spécifie un code qui, déchiffré avec la clé publique, donne une suite comportant un texte de référence prédéterminé en tant que sous-suite. Même dans le cas où un certain code choisi arbitrairement donnerait au déchiffrage une suite qui contiendrait, en tant que l'une de ses parties, le texte de référence prédéterminé AMERICAN EXPRESS, il faudrait que ce texte de référence prédéterminé figure en position correcte dans la combinaison décryptée totale du mot de passe et du texte de référence, et la probabilité que cela arrive est plus faible encore que celle de deviner un code qui donnerait au déchiffrage une suite complète contenant le texte de référence AMERICAN EXPRESS dans une quelconque position arbitraire.

On notera que ce système d'authentification peut être utilisé par un grand nombre d'émetteurs de cartes. Si chaque émetteur a sa propre paire de clés publique-secrète et son propre texte de référence, chaque carte portera le texte de référence ou une autre identification de l'émetteur et chaque terminal de transactions contiendra en mémoire la série complète de textes de référence d'émetteurs acceptables et de clés publiques. Pour plus de commodité, la carte peut aussi porter la clé publique appropriée, bien que cette clé, de même que le texte de référence, doive être composée comme un élément d'une série mémorisée dans le terminal. Il est même possible qu'une même carte soit utilisée en commun par plusieurs émetteurs, cette carte contenant plusieurs mots de code

chiffrés, correspondant chacun à un émetteur particulier et régissant l'accès à une valeur de crédit ou à une acceptabilité mémorisée dans une section particulière de la mémoire de la carte. Une identification de chaque émetteur est nécessaire et, de même que dans le cas d'une carte d'émetteur unique, le texte de référence de l'émetteur peut remplir cette fonction. Pour des raisons de commodité, la carte peut aussi porter la clé publique de chaque émetteur.

D'autres buts, caractéristiques et avantages de la présente invention apparaîtront à l'examen de la description détaillée qui suit, donnée en référence aux dessins ci-annexés.

La fig. 1 représente les composants utilisés dans un système complet suivant la présente invention.

La fig. 2 montre la forme d'un terminal qui peut être utilisé dans le système de la présente invention.

Les fig. 3A et 3B illustrent respectivement une solution insatisfaisante de l'état antérieur de la technique pour le problème des falsifications et la solution de la présente invention, offrant un degré élevé de sécurité.

La fig. 4 représente symboliquement les détails d'une carte intelligente et d'un terminal d'initialisation, lors de l'utilisation de ce dernier pour initialiser la carte.

La fig. 5 représente symboliquement les détails d'une carte intelligente et d'un terminal de transactions, lors de l'utilisation de ce dernier pour l'exécution d'une transaction sous le contrôle de la carte.

La fig. 6 est un organigramme qui représente l'opération d'initialisation d'une carte.

La fig. 7 est un organigramme qui représente l'opération d'exécution d'une transaction avec une carte intelligente.

Avant d'en venir à la description détaillée de la présente invention, on présentera un bref résumé des principes de la cryptographie à clé publique. Sous sa forme la plus simple et telle qu'elle a été conçue à l'origine pour la transmission de messages sur des canaux de communications, chaque utilisateur calcule ou se

voit attribuer une paire de clés complémentaires. De façon générale, les deux clés sont désignées par les symboles E et D et elles sont utilisées toutes les deux pour régir des opérations sur des suites alphanumériques représentées sous forme de nombres. Dans le système connu de Rivest-Shamir-Adleman (RSA), les deux clés sont commutatives, en ce sens que si un texte original est chiffré avec la clé E, un traitement du texte chiffré sous le contrôle de la clé D aboutira au texte original, tandis que des chiffrages, d'abord avec la clé D, puis avec la clé E aboutissent également au texte original. La sécurité des systèmes à clé publique tient à l'extrême difficulté du calcul pour trouver l'une des clés à partir de l'autre.

Dans le cas usuel, un participant auquel des messages doivent être envoyés publie sa clé E dans un répertoire central. Quiconque veut lui transmettre un message transforme ou chiffre celui-ci avec la clé E. La clé D n'est connue que du participant qui est en mesure de décrypter tout message qui lui arrive à l'aide de cette clé. Par contre, toute autre personne qui aurait accès au message chiffré transmis le trouverait totalement inintelligible, car en l'absence de clé D, le message transmis ne peut pas être déchiffré. Les symboles E et D sont généralement utilisés pour la raison que l'une des clé sert au chiffrage ("Encryption" en anglais) et l'autre pour le déchiffrage ("Decryption"), bien que leurs rôles puissent être intervertis, comme on l'a vu ci-dessus. La clé E est appelée "clé publique" parce qu'elle est publiée afin que le monde entier sache comment chiffrer des messages en vue de leur transmission secrète au détenteur de la paire de clés. La clé D est la "clé privée", car elle n'est connue que du détenteur particulier de la paire de clés.

Si le secret n'est pas une préoccupation, mais qu'à la place, le but recherché est l'authentification, le participant qui émet le message utilise sa clé privée pour le transformer. C'est donc sa clé D, utilisée ordinairement pour le decryptage, qui sert pour authentifier (chiffrer) un message. Le participant qui reçoit le message chiffré utilise la clé publique E de l'émetteur

pour décrypter le message qui arrive, afin de le transformer en le texte original. Pourvu que le message chiffré qui arrive soit maintenu à l'abri des indélicatesses, le participant en réception peut "vérifier" l'anthenticité du message reçu. L'utilisation de la clé publique de l'émetteur pour décrypter le message qui arrive n'aboutit à un texte intelligible que si le message original a été chiffré avec la clé privée de l'émetteur. Etant donné que l'émetteur est la seule personne qui a connaissance de sa clé privée, la réception et la conservation d'un message chiffré qu'il est possible de transformer en un texte intelligible en utilisant la clé publique de l'émetteur servent de preuve que c'est vraiment lui qui a envoyé le message.

Alors que le chiffrage d'un message avec la clé publique du destinataire assure le secret et que le chiffrage d'un message avec la clé privée de l'envoyeur assure l'authenticité, il n'y a aucun moyen, dans le premier cas, de prouver qu'un message qui arrive est authentique et il n'y a aucun moyen, dans le second cas, d'assurer le secret. Dans le premier cas, il n'y a aucun moyen, pour le destinataire, de savoir si le participant de qui le message est censé provenir l'a réellement émis, puisque le monde entier a accès à la clé publique du destinataire. Dans le second cas, étant donné que le monde entier connaît la clé publique de l'envoyeur, n'importe qui peut déchiffrer le message transmis s'il y a accès. La manière d'assurer à la fois le secret et l'authenticité consiste, pour l'envoyeur, de chiffrer doublement le message avec sa clé privée et avec la clé publique du destinataire et, pour le destinataire, de déchiffrer doublement le message avec sa clé privée et avec la clé publique de l'envoyeur. Grâce à la propriété de commutativité de chaque paire de clés, le message qui a subi un double déchiffrage sera le même que le texte original avant le double chiffrage. Le secret est assuré par le fait que le destinataire est le seul à avoir sa clé privée qui est nécessaire pour un décryptage partiel. L'authentification est assurée par le fait que, quoique le monde entier ait la clé publique de l'envoyeur, un message transmis qui peut donner au déchiffrage un texte ayant une

signification n'a pu être chiffré que par le détenteur de la clé privée de l'envoyeur.

Etant donné qu'en fait, l'envoyeur peut utiliser sa clé privée D à des fins de chiffrage, sa clé publique E étant utilisée par un destinataire pour le décryptage, les symboles D et E ne désignent pas toujours forcément des clés de décryptage et de chiffrage respectivement. L'une ou l'autre peut servir pour le chiffrage et l'une ou l'autre peut être utilisée pour le décryptage. Toutefois, ce sont les symboles qui ont été adoptés. Ce qui est commun à toute paire de clés dans un "système cryptographique à clé publique", c'est que l'une des clés est publique (ou, tout au moins, le détenteur de la paire de clés ne s'inquiète pas réellement si elle devient publique) et que l'autre est privée; la clé publique est ici appelée clé E et la clé privée est ici appelée clé D. Ce qui est également commun à tous ces systèmes cryptographiques, c'est que ni l'une ni l'autre des clés ne peut être déterminée à partir de l'autre.

Dans un système cryptographique à clé publique utilisant le système RSA, un message à transmettre est d'abord élevé à la puissance S. Le message chiffré final est le message original élevé à la puissance S, modulo R. C'est-à-dire qu'il n'est effectivement transmis que le reste après que le message original a été élevé à la puissance S et divisé à répétition par R. Le nombre R peut avoir typiquement une longueur de 300 bits et la puissance S à laquelle le message original est élevé a typiquement une longueur de 50 bits. Naturellement, la longueur de chaque message doit être inférieure à la longueur de R, car le message chiffré doit avoir au moins autant de bits que le message original. Les nombres S et R constituent ensemble la clé publique de l'utilisateur qui est publiée. La clé privée comprend les nombres T et R Le message qui arrive est élevé à la puissance T, puis divisé à répétition par le nombre R, jusqu'à ce que le reste soit inférieur à R. Ce reste est le message décrypté.

L'utilisateur garde secret son code privé, le nombre T étant la partie importante du secret, puisque le nombre R est connu.

Comme on l'a déjà vu, si la cryptographie à clé publique marche, c'est parce qu'en possédant la clé S, il est pratiquement impossible de déterminer la clé T. On trouvera, dans la littérature précitée, non seulement une description de la base de la cryptographie à clé publique, mais aussi la manière par laquelle des clés privées et publiques peuvent être créées par paires.

La fig. 1 représente les composants de base d'un système construit suivant les principes de la présente invention. Le numéro 12 désigne une carte intelligente, dont un exemplaire est délivré à chaque usager du système. Les contacts permettant à un terminal d'avoir accès à la carte sont indiqués symboliquement à l'angle supérieur gauche de l'enveloppe de la carte, ces contacts traversant l'enveloppe vers la mémoire et les circuits logiques et/ou le microprocesseur contenus à l'intérieur de l'enveloppe. Le terminal 10a est le terminal d'initialisation, utilisé par l'émetteur de cartes; chaque carte d'utilisateur doit être initialisée avec, entre autres choses, un mot de passe d'utilisateur.

Le numéro 10b désigne un terminal de transactions qui peut être utilisé, après insertion d'une carte d'utilisateur, pour l'exécution d'une transaction. Le numéro 13 a simplement trait à la manière dont la transaction est enregistrée. L'enregistrement peut être mémorisé sur place ou il peut être transmis ailleurs. De même, il peut être imprimé ou même mémorisé dans la carte d'utilisateur.

La fig. 2 montre la forme générale d'un terminal. Ce terminal peut être, soit le terminal d'initialisation 10a de la fig. 1, soit le terminal de transactions 10b de la fig. 1; la seule différence réside dans les détails du traitement qui y est effectué, comme on le verra ci-après. Comme le montre la fig. 2, le terminal comprend un dispositif d'affichage 14 pour la visualisation de messages et d'instructions destinées à l'utilisateur de la carte, une fente 16 dans laquelle une carte 12 est insérée et un clavier 18. Le clavier sert à la fois à l'introduction des informations nécessaires pour la transaction et à celle d'un mot de passe d'utilisateur.

La fig. 3B montre symboliquement comment la falsification de

cartes ou le "bernement" d'un terminal (et spécialement d'un terminal sans surveillance) sont empêchés d'après les principes de la présente invention. Le système de l'invention doit être confronté à un système représentatif de l'état antérieur de la technique, illustré de façon semblable sur la fig. 3A, ce système de l'état antérieur de la technique étant commercialisé sous le nom de marque "Identikey" et étant bien connu des spécialistes.

Le système "Identikey" est actuellement utilisé dans le secteur bancaire. Un utilisateur choisit son propre mot de passe secret et le garde en mémoire. Il est également attribué, à l'utilisateur, deux numéros supplémentaires, qui peuvent être enregistrés l'un et l'autre sur une carte d'identification - son numéro de compte et son numéro d'identification. Ces deux derniers numéros sont non secrets, non pas dans le sens qu'ils sont inscrits sur un registre public (bien que l'un d'eux ou l'un et l'autre peuvent être imprimés effectivement sur la carte de l'utilisateur), mais en ce sens qu'il n'est généralement pas possible d'éviter qu'au moins un guichetier de la banque prenne connaissance de ces deux numéros. On doit donc admettre que les deux numéros sont non secrets.

Lorsque l'identité de l'utilisateur doit être établie pour qu'une transaction puisse être exécutée, le numéro de compte de l'utilisateur est introduit à partir de sa carte (ou manuellement) et l'utilisateur introduit son mot de passe dans le terminal à l'aide du clavier (à titre de mesure de sécurité à un premier niveau, le terminal peut transmettre le mot de passe à la carte et ce n'est qu'après que la carte a signalé au terminal qu'il y a une concordance des mots de passe, que le terminal a accès au numéro de compte sur la carte). Le terminal effectue alors une transformation non linéaire et effectivement irréversible sur la combinaison du numéro de compte et du mot de masse, et il produit un numéro d'identification de contrôle. Le numéro d'identification de l'utilisateur est également introduit dans le terminal, soit par transfert à partir de la carte, soit par introduction manuelle. Ce n'est que si le numéro d'identification mémorisé sur la carte concorde avec le numéro d'identification de contrôle produit dans

le terminal, que ce dernier donne l'autorisation d'exécution de la transaction. Le dessin montre que la comparaison des deux numéros d'identification aboutit, soit à l'acceptation de la carte et à l'exécution de la transaction, soit au rejet de la carte (et, le cas échéant, à sa destruction et/ou à sa confiscation).

Il est admis que la transformation F est irréversible, en ce sens que si le numéro d'identification d'un utilisateur est connu et si son numéro de compte est également connu, une connaissance de la transformation F ne suffira pas pour permettre à un individu, même versé dans les mathématiques, de déterminer le mot de passe qui est associé à la carte. Ainsi, un voleur par exemple, même s'il connaît le numéro d'identification et le numéro de compte d'un utilisateur, ne sera pas en mesure de déterminer son mot de passe.

Toutefois, en supposant que l'usage des terminaux de transactions soit largement répandu, le système manque de sécurité, car il n'y a pas moyen d'éviter que la transformation F soit généralement connue. Tout ce qu'un falsificateur a à faire, c'est de choisir un mot de passe arbitraire et un numéro de compte arbitraire et d'utiliser la transformation F sur ces numéros pour en déduire un numéro d'identification. Il peut alors introduire le numéro de compte arbitraire et le numéro d'identification qui en dérive dans un quelconque terminal pour établir son identité. Naturellement, cela ne permet pas au falsificateur de se faire passer indûment pour un individu particulier auquel des numéros de compte et d'identification ont déjà été attribués. Pour personnifier cet individu, le falsificateur doit créer un mot de passe en harmonie avec les numéros de compte et d'identification connus. Certaines limitations du système rendent cette opération plus facile que d'inverser la fonction F, mais cela reste une tâche qui exige des calculs longs et compliqués. Pour ces raisons, le système "Identikey" offre une sécurité acceptable dans des applications "en connexion" avec l'ordinateur, dans lesquelles la série de numéros d'identification en vigueur est disponible à titre de référence, mais non dans des applications en autonome, dans lesquelles il

n'est pas possible de consulter une telle liste.

Dans le système de la présente invention illustré par la fig. 3B, il est attribué, à l'utilisateur, un mot de passe secret ainsi qu'un numéro d'identification non secret. Ce numéro d'identification est le code, mémorisé sur la carte par le terminal d'initialisation, c'est-à-dire la combinaison du mot de passe secret, choisi par l'utilisateur, et du texte de référence AMERICAN EXPRESS, chiffrés ensemble au moyen de la clé privée de l'émetteur de cartes. A l'aide de la clé publique E associée, qui est mémorisée dans le terminal, le numéro d'identification de l'utilisateur est décrypté en deux suites, consistant respectivement en le mot de passe de l'utilisateur et en le texte AMERICAN EXPRESS. Le terminal demande à l'utilisateur d'introduire son mot de passe secret (là encore, des dispositions peuvent être prises pour que le terminal n'ait accès à la carte qu'après que le mot de passe correct a été introduit, de même que dans l'état antérieur de la technique). Le terminal compare alors le mot de passe introduit et le texte de référence AMERICAN EXPRESS d'usage universel avec les deux parties du numéro d'identification décrypté. Ce n'est que si les deux parties concordent que le terminal passe à l'exécution d'une transaction.

De même qu'il est admis qu'un falsificateur chevronné puisse connaître la transformation F de la fig. 3A, il est admis qu'il puisse connaître la clé publique E de la fig. 3B, puisqu'il y a beaucoup de terminaux de transactions en service et qu'il est relativement simple de prendre connaissance de la clé publique. Supposons que le falsificateur essaie de faire, avec le système de la fig. 3B, quelque chose de comparable à ce qu'il peut faire avec le système de la fig. 3A, à savoir choisir un numéro d'identification arbitraire, le décrypter en utilisant la clé publique E qu'il connaît, puis utiliser les résultats décryptés pour créer une "boîte noire" ou une carte falsifiée qui soit capable de berner un terminal de transactions. Un terminal ne peut être "berné" que si le décryptage aboutit à un mot de passe et au texte du message AMERICAN EXPRESS. Au cas où un numéro d'identification

choisi arbitrairement donne vraiment, après décryptage avec la clé publique E, le texte du message AMERICAN EXPRESS en position correcte (par exemple à la fin) et, en plus, une certaine combinaison arbitraire de lettres et de chiffres, cette dernière combinaison serait le mot de passe que le falsificateur pourrait ensuite utiliser dans sa "boîte noire" ou en l'introduisant sur le clavier. Mais il y aurait une probabilité infinitésimale pour que le choix arbitraire d'un numéro d'identification aboutisse, au décryptage de celui-ci, au texte du message prédéterminé en position correcte, accompagné d'une certaine combinaison arbitraire de caractères. Ainsi, la connaissance de la clé publique E n'est pas suffisante pour permettre à un falsificateur de choisir un numéro d'identification (la combinaison d'un mot de passe et du texte du message AMERICAN EXPRESS, chiffrée par la clé secrète de l'émetteur de cartes) qui donne lieu à une transaction. Le seul moyen possible de choisir un numéro d'identification qui donne, au décryptage avec la clé publique, une partie mot de passe et une partie texte du message prédéterminé, est d'utiliser la clé privée dans l'opération de chiffrage, et le falsificateur n'a aucune posssibilité d'accès à la clé privée.

Il est essentiel que le résultat du décryptage comprenne à la fois une partie mot de passe et une partie texte de référence prédéterminé. Si le cryptogramme mémorisé sur la carte ne comprenait qu'un mot de passe, le falsificateur pourrait choisir un numéro d'identification arbitraire, le décrypter avec la clé publique E et utiliser le résultat en tant que mot de passe; la mise en mémoire du numéro d'identification choisi arbitrairement dans la "boîte noire", en vue de son utilisation dans un terminal en tant que code chiffré sur une carte, aboutirait toujours à une comparaison couronnée de succès lors de l'introduction, par le falsificateur, du mot de passe déduit à l'aide de la clé publique E. De même, si le code sur le carte ne comprenait rien de plus que le texte du message AMERICAN EXPRESS chiffré avec la clé privée D, tout ce que le falsificateur aurait à faire, c'est de déterminer le même cryptogramme qui est mémorisé sur chaque carte

et de l'utiliser dans sa "boîte noire". Le décryptage dans un terminal quelconque avec la clé publique E donnerait nécessairement le texte de référence AMERICAN EXPRESS. Ce qui est nécessaire pour la sécurité, c'est de mémoriser dans une carte le code qui est un cryptogramme, créé avec la clé privée D, d'une combinaison d'un mot de passe et d'un texte de référence prédéterminé. Il n'y a aucune possibilité pour qu'un falsificateur - même s'il connaît la clé publique E - puisse choisir un numéro d'identification arbitraire ou un cryptogramme à mémoriser sur une carte, qui donne au décryptage un certain mot de passe arbitraire, accompagné du texte de référence prédéterminé dans la position correcte dans les suites enchaînées.

La fig. 4 représente, du côté gauche, les composants contenus dans la carte intelligente 12 elle-même. Ces composants sont indiqués simplement sous la forme de schéma-bloc, eu égard au fait que les constructions de cartes intelligentes sont connues en soi dans la technique. La mémoire 28 est divisée en six segments. L'un des segments de la mémoire contient le mot de passe d'utilisateur. Ce mot de passe est choisi par l'utilisateur (de telle sorte qu'il puisse s'en souvenir), il est mis en mémoire dans la carte par le terminal d'initialisation de l'émetteur de cartes et il est ensuite utilisé, sous le contrôle d'un quelconque terminal de transactions, pour vérifier si l'individu qui utilise la carte est bien l'utilisateur autorisé, en exigeant que le mot de passe que cet individu introduit concorde avec celui qui est mémorisé dans la carte.

La mémoire contient également un mot de passe d'émetteur de cartes. C'est un mot de passe que le fabricant de cartes mémorise dans la carte, mot qui n'est connu que du fabricant et de l'émetteur de cartes. Comme on le verra ci-après, une carte dérobée au fabricant ne peut pas être initialisée par un voleur, car celui-ci ne connaît ordinairement pas le mot de passe d'émetteur qu'un terminal d'initialisation exige pour initialiser une carte d'utilisateur.

Le segment suivant de la mémoire contient un code qui est un

cryptogramme d'un enchaînement de deux suites, l'une étant le mot de passe d'utilisateur et l'autre étant un texte de référence tel que AMERICAN EXPRESS. La clé privée D de l'émetteur de cartes est utilisée pour chiffrer les suites enchaînées dans le terminal d'initialisation de l'émetteur.

Le "programme enregistré " est simplement le code objet qui régit le fonctionnement du microprocesseur 30. Le segment de la mémoire qui contient des "informations générales" est facultatif, mais il peut contenir des informations à ajouter en tant que partie de l'en-tête d'un quelconque message de transaction qui est engendré. Par exemple, il pourra contenir le nom et l'adresse de l'utilisateur.

Les cinq segments de la mémoire 28 qui ont été décrits jusqu'ici peuvent être du type mémoire fixe, en ce sens qu'après que la carte a été initialisée, les informations contenues dans ces segments de la mémoire n'ont jamais besoin d'être modifiées (certaines parties de la mémoire fixe, notamment le programme enregistré, peuvent être écrites par le fabricant de cartes, tandis que d'autres parties de la mémoire peuvent être introduites une fois pour toutes par le terminal d'initialisation; typiquement, le mot de passe, le cryptogramme de code et les informations générales peuvent constituer le contenu d'une mémoire fixe programmable). La seule partie de la mémoire qui doit être à accès sélectif est la "mémoire de travail", c'est-à-dire la partie de la mémoire qui est utilisée par le microprocesseur lors du traitement. Bien que cela n'ait pas été indiqué sur les dessins, il est bien entendu que la fente dans laquelle la carte est insérée, dans l'un et l'autre types de terminal, contient des broches pour transmettre l'énergie à des broches correspondantes sur la carte. Typiquement, la carte nécessite deux sources d'énergie : 5 volts pour l'alimentation des circuits logiques TTL sur plaquette ou du microprocesseur, et 24 volts pour charger les segments PROM (mémoire fixe programmable) de la mémoire 28, de façon connue en soi (le terminal de transaction, comme on le verra ci-après, n'a pas besoin de fournir d'énergie sous 24 volts).

La carte contient aussi une section d'entrée/sortie (I/O) 32 qui sert d'interface avec un terminal 10. La fonction principale de la section d'entrée/sortie est la conversion parallèle-série. Une seule broche sur la carte sert à l'émission et à la réception de données en série. Un jeu de lignes de commande est prévu pour la transmission aller-retour des informations de synchronisation et de commande entre la carte et le terminal.

La carte contient également des bus classiques de données, d'adresses et de commande pour l'interconnexion du microprocesseur, de la mémoire et des sous-systèmes d'entrée/sortie.

De même, le terminal d'initialisation 10a de la fig. 4 comprend une section d'entrée/sortie (I/O) 34, un microprocesseur 36 et une mémoire 40, interconnectés par des bus classiques de données, d'adresses et de commande. Le clavier 18 est relié aux trois bus de telle manière qu'un mot de passe d'utilisateur puisse être introduit, ainsi que pour l'introduction de toute autre information générale voulue. Une commande d'affichage 38, de type classique, constitue l'interface entre le dispositif d'affichage 14 du terminal et les trois bus, de façon connue en soi dans la technique.

La mémoire 40 contient cinq types d'informations. La mémoire de travail est à accès sélectif et c'est la mémoire utilisée par le microprocesseur au cours du traitement. Les quatre autres segments de la mémoire peuvent être du type mémoire fixe. Le"programme enregistré principal"commande la majeure partie du traitement qui sera décrit ci-après. La partie de la mémoire désignée par "texte de référence" contient la phrase AMERICAN EXPRESS dans le cas de l'exemple décrit ci-dessus, c'est-à-dire le texte de référence qui constitue l'une des parties de l'enchaînement qui est chiffré avec la clé privée D. Il est prévu un programme enregistré supplémentaire pour chiffrer la combinaison du mot de passe choisi par l'utilisateur et du texte du message fixe, avec la clé privée D de l'émetteur de cartes (à proprement parler, cette partie de la mémoire contient simplement l'un parmi plusieurs sous-programmes et elle peut être considérée comme faisant partie du programme enregistré principal). La mémoire 40 contient aussi le mot de passe

de l'émetteur de cartes, dont la fonction sera décrite brièvement.

L'organigramme de la fig. 6 montre comment une carte d'utilisateur est initialisée (le code objet pour l'exécution de l'opération d'initialisation ne figure pas sur les dessins, car tout spécialiste sera en mesure, à partir de l'organigramme, d'écrire un programme source qui, après assemblage, fournira le code objet pour la commande du microprocesseur). Au début de l'opération d'initialisation, après que la carte d'utilisateur a été insérée dans la fente prévue à cet effet dans le terminal d'initialisation, le terminal lit le mot de passe de l'émetteur de cartes dans sa mémoire et le transmet à la carte. Le mot de passe d'émetteur qui est ainsi transmis à la carte est comparé par le microprocesseur 30 avec le mot de masse d'émetteur qui est stocké dans la mémoire de la carte. Le résultat de la comparaison est transmis au terminal. Si les deux mots de passe ne concordent pas, l'opération d'initialisation est suspendue prématurément; autrement, elle se poursuit comme indiqué dans l'organigramme.

Cette comparaison de mots de passe est classique dans la technique des cartes intelligentes. Le fabricant de cartes enregistre un mot de passe d'émetteur différent sur chacune des cartes numérotées en série qu'il fabrique. Sans cette mesure de sécurité, en cas de détournement d'un plein camion de cartes, le voleur pourrait les initialiser et les utiliser. Par un moyen de transport différent de haute sécurité, le fabricant envoie à l'émetteur de cartes la liste de mots de passe d'émetteur correspondant aux cartes numérotées en série. De cette manière, l'auteur du détournement d'un plein camion de cartes ne peut pas utiliser celles-ci, puisqu'il ne connaît pas les mots de passe d'émetteur qui sont nécessaires pour initialiser les cartes.

Pour en revenir à la fig. 6, le terminal demande alors à l'utilisateur d'introduire un mot de passe, au moyen du dispositif d'affichage 14 prévu sur le terminal d'initialisation. Si on laisse l'utilisateur choisir son propre mot de passe, c'est pour que son choix porte sur un mot qu'il ne risque pas d'oublier. Le mot de passe est alors transmis à la carte, pour y être enregistré

dans la mémoire 28 en tant que mot de passe d'utilisateur.

Le terminal utilise alors la clé privée D pour chiffrer un message qui comporte deux parties, le mot de passe d'utilisateur précédemment introduit et le texte de référence prédéterminé, le même texte de référence étant utilisé dans le chiffrage de chaque carte à initialiser. La clé privée D qui est utilisée est la clé privée qui est associée à la clé publique d'une paire de clés de système cryptographique à clé publique (les techniques pour la création de clés privées et publiques appariées sont connues en soi; tout ce qui importe pour comprendre la présente invention est de voir comment une telle paire de clés est utilisée). L'enchaînement de suites chiffré est ensuite envoyé par le terminal à la carte où il est mémorisé, avec toute autre information générale qui peut être introduite par le clavier, notamment le nom et l'adresse de l'utilisateur.

La carte intelligente 12 a été également représentée sur la fig. 5, cette fois en interface avec un terminal de transactions 10 b. La carte elle-même est la même que la carte représentée sur la fig. 4 et son interface avec le terminal est réalisée de la même manière. Le terminal de transactions 10b contient les mêmes composants de base que le terminal d'initialisation 10a sur la fig. 4. La différence majeure est que le terminal de transactions comporte un dispositif supplémentaire 13 de mémorisation ou de transmission, associé à un circuit d'entrée/sortie 54 qui le relie aux trois bus du système. Comme on l'a vu précédemment à propos de la fig. 1, un enregistrement représentatif d'une transaction est mémorisé, transmis, imprimé, etc. Il va de soi que la mémoire 40 du terminal de transactions est différente de la mémoire comparable du terminal d'initialisation, puisque des fonctions différentes doivent être remplies. Le terminal de transactions comporte une mémoire de travail et un programme enregistré principal. Fait partie de ce programme un sous-programme qui commande un décryptage par clé publique du code chiffré mémorisé sur toute carte d'utilisateur à laquelle le terminal a accès. C'est ce sous-programme qui décrypte la suite enchaînée chiffrée que porte la carte d'utilisa-

teur, pour en tirer les parties mot de passe et texte de référence. La mémoire 40 contient aussi un segment qui garde le texte de référence universel, par exemple AMERICAN EXPRESS, de telle manière que le terminal puisse vérifier si le message décrypté comprend bien deux parties qui concordent respectivement avec le mot de passe d'utilisateur, introduit par le clavier, et avec le texte de message universel. Il va de soi que la mémoire 40 contient également un programme enregistré pour l'exécution effective d'une transaction voulue, après qu'il a été constaté qu'une carte a été insérée dans la machine par le porteur légitime d'une carte valide.

La fig. 7 est l'organigramme qui caractérise le fonctionnement d'un terminal de transactions. La première phase est l'introduction du mot de passe par le détenteur de la carte. Eu égard au fait que les détenteurs de carte introduisent fréquemment de manière incorrecte leurs mots de passe respectifs, il leur est accordé quatre essais pour introduire correctement leur mot de passe par l'intermédiaire du clavier. Un compte j est réglé à 1, puis le terminal demande, au moyen du dispositif d'affichage, que l'utilisateur introduise son mot de passe. Le terminal transmet alors le mot de passe introduit à la carte, où il est comparé avec le mot de passe d'utilisateur mémorisé. Il est préférable que la comparaison soit effectuée sur la carte, plutôt que dans le terminal, pour des raisons de sécurité : en effet, il n'y a aucun moyen, pour quelqu'un qui a "tripoté" dans le terminal, d'avoir accès au mot de passe d'utilisateur. Si le mot de passe introduit ne concorde pas avec celui de la carte, le compte j est augmenté, puis il est comparé avec un compte maximal de 5. Si j est égal à 5, cela indique qu'un utilisateur a essayé d'introduire un mot de passe correct à quatre reprises et qu'il n'a pas réussi. Il est donc supposé qu'il n'est pas le détenteur de la carte et le déroulement de l'opération complète est suspendu, comme indiqué dans l'organigramme de la fig. 7. Par contre, si c'est par inadvertance qu'il a introduit le mauvais mot de passe, il lui est donné trois autres chances pour rectifier le tir. Dans la mesure où le mot

de passe correct de l'utilisateur de la carte est introduit correctement dans les limites de quatre tentatives, le traitement se poursuit.

Le terminal commande alors à la carte de lui transmettre le cryptogramme combiné du mot de passe d'utilisateur et du texte de référence prédéterminé, qui est mémorisé dans la carte. La clé publique E est utilisée dans le terminal pour décrypter le code chiffré mémorisé dans la carte et le résultat doit être un enchaînement du mot de passe d'utilisateur et du texte de référence AMERICAN EXPRESS, comme on l'a vu précédemment. La première partie du message décrypté, c'est-à-dire la partie mot de passe d'utilisateur, est comparée avec le mot de passe introduit, pour voir si elles concordent. S'il n'en est pas ainsi, l'opération est suspendue. Si elles concordent, le terminal compare la partie texte de message décrypté avec le texte de référence prédéterminé qui est mémorisé dans le terminal, AMERICAN EXPRESS. Là encore, s'il y a non-concordance, la transaction est suspendue. La transaction n'est exécutée que si les deux parties du code chiffré décrypté concordent respectivement avec le mot de passe d'utilisateur secret, introduit par l'utilisateur, et le texte de référence prédéterminé.

L'invention a été décrite à propos d'une forme de réalisation particulière, mais il est bien entendu que cette forme de réalisation n'est qu'une illustration de l'application des principes de l'invention. De nombreuses modifications peuvent y être apportées et d'autres dispositions peuvent être imaginées, sans que l'on s'écarte pour autant de l'esprit et de la portée de l'invention.

- REVENDICATIONS -

1. Système pour permettre à des utilisateurs autorisés de cartes intelligentes portatives d'exécuter des transactions au moyen d'au moins un terminal de transactions, caractérisé en ce qu'il comprend une multiplicité de cartes intelligentes d'utilisateur, dans chacune desquelles est mémorisé un code qui est le cryptogramme d'une combinaison d'un mot de passe attribué à l'utilisateur respectif et d'un texte de référence qui est commun à tous les utilisateurs, les codes mémorisés dans toutes les cartes ayant été chiffrés avec la même clé privée qui est associée à la clé publique d'une paire de clés d'un système cryptographique à clé publique ; et au moins un terminal de transactions qui comporte des moyens pour permettre à un utilisateur de carte d'y introduire un mot de passe, et des moyens pour commander : 1) l'extraction du code mémorisé dans une carte insérée, 2) le décryptage du code extrait à l'aide de ladite clé publique pour en tirer une partie mot de passe et une partie texte, 3) les comparaisons de la partie mot de passe ainsi obtenue avec le mot de passe introduit et de la partie texte avec ledit texte commun de référence, et 4) l'exécution d'une transaction, seulement si ces deux comparaisons sont couronnées de succès.

2. Système selon la revendication 1, caractérisé en ce que chacune des cartes contient en outre des moyens pour mémoriser par elle-même le mot de passe respectif, et des moyens pour recevoir un mot de passe fourni par le terminal et pour comparer le mot de passe fourni avec le mot de passe mémorisé, les moyens de commande du terminal ne commandant l'extraction du code mémorisé dans une carte insérée que dans le cas où la comparai-

son des mots de passe est couronnée de succès.

3. Système selon la revendication 1 ou 2, caractérisé en ce qu'il comprend plusieurs terminaux de transactions, dont l'un au moins est sans surveillance.

4. Système selon l'une quelconque des revendications 1 à 3, caractérisé en outre en ce qu'il comprend au moins un terminal pour initialiser une carte intelligente d'utilisateur, ce terminal d'initialisation comportant des moyens pour affecter un mot de passe à un utilisateur dont la carte doit être initialisée, des moyens pour former un code en chiffrant, avec ladite clé privée, la combinaison du mot de passe affecté et dudit texte de référence commun, et des moyens pour commander la mémorisation du code ainsi formé dans la carte.

5. Système selon la revendication 4, caractérisé en ce que le terminal d'initialisation commande en outre la mémorisation séparée du mot de passe assigné dans la carte.

6. Terminal pour l'initialisation de cartes intelligentes portatives, destinées à être utilisées avec au moins un terminal de transactions, chacune de ces cartes intelligentes comportant une mémoire, caractérisé en ce qu'il comprend des moyens pour affecter un mot de passe à un utilisateur dont la carte doit être initialisée, des moyens pour former un code qui est le cryptogramme d'une combinaison du mot de passe affecté et d'un texte de référence qui est commun à tous les utilisateurs, le code pour chaque utilisateur étant formé à l'aide de la même clé privée qui est associée à la clé publique d'une paire de clés d'un système cryptographique à clé publique, et des moyens pour commander la mémorisation du code respectif ainsi formé dans une carte d'utilisateur.

7. Terminal d'initialisation selon la revendication 6, caractérisé en ce qu'il comprend en outre des moyens pour commander la mémorisation séparée du mot affecté respectif dans une carte d'utilisateur.

8. Carte intelligente portative, destinée à être utilisée pour exécuter des transactions au moyen d'au moins un terminal de transactions, caractérisée en ce qu'elle comprend une enveloppe, une mémoire à l'intérieur de cette enveloppe pour mémoriser un code, ce code étant le cryptogramme d'une combinaison d'un mot de passe affecté à l'utilisateur de carte

respectif et d'un texte de référence qui est commun à tous les autres utilisateurs de cartes semblables, ce code ayant été chiffré avec la clé privée qui est associée à la clé publique d'une paire de clés d'un système cryptographique à clé publique, et des moyens pour permettre d'avoir accès au code mémorisé depuis l'extérieur de la carte.

9. Carte intelligente portative selon la revendication 8, caractérisée en ce que la mémoire mémorise en outre séparément le mot de passe.

10. Carte intelligente portative selon la revendication 9, caractérisée en ce qu'elle comprend en outre des moyens pour recevoir un mot de passe qui doit être comparé avec le mot de passe mémorisé et pour comparer ces mots de passe.

11. Carte intelligente portative selon la revendication 10, caractérisée en ce qu'elle comprend un outre des moyens pour commander l'extraction du code mémorisé.

12. Carte intelligente portative selon la revendication 11, caractérisée en ce que le code mémorisé n'est extrait que si la comparaison est couronnée de succès.

13. Carte intelligente portative selon la revendication 8, caractérisée en ce qu'elle comprend en outre des moyens pour commander l'extraction du code mémorisé.

14. Carte intelligente portative selon la revendication 8, caractérisée en ce que la mémoire mémorise plusieurs codes, associés chacun à un fournisseur de services différent.

15. Carte intelligente portative selon la revendication 14, caractérisée en ce que la mémoire mémorise, en association avec chacun desdits codes multiples, une identification du fournisseur de services respectif.

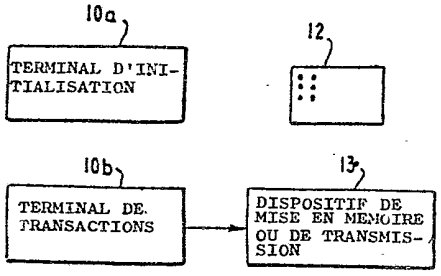


FIG. 1

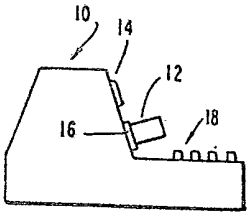


FIG. 2

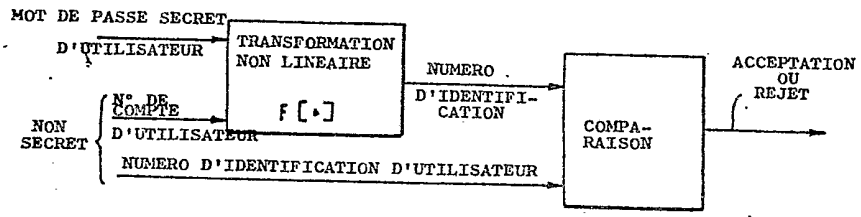


FIG. 3A

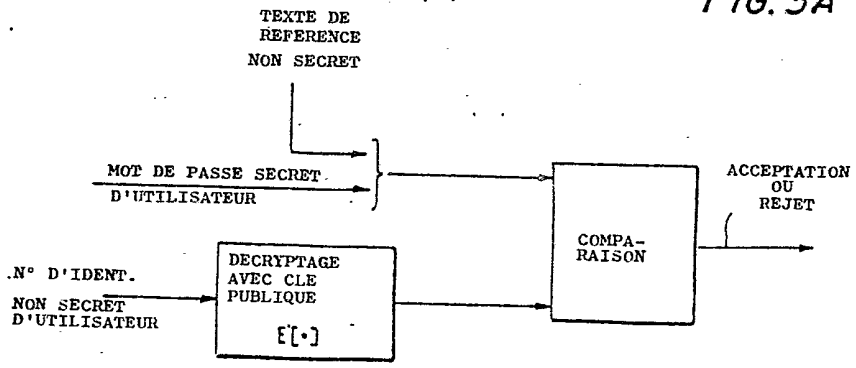


FIG. 3B

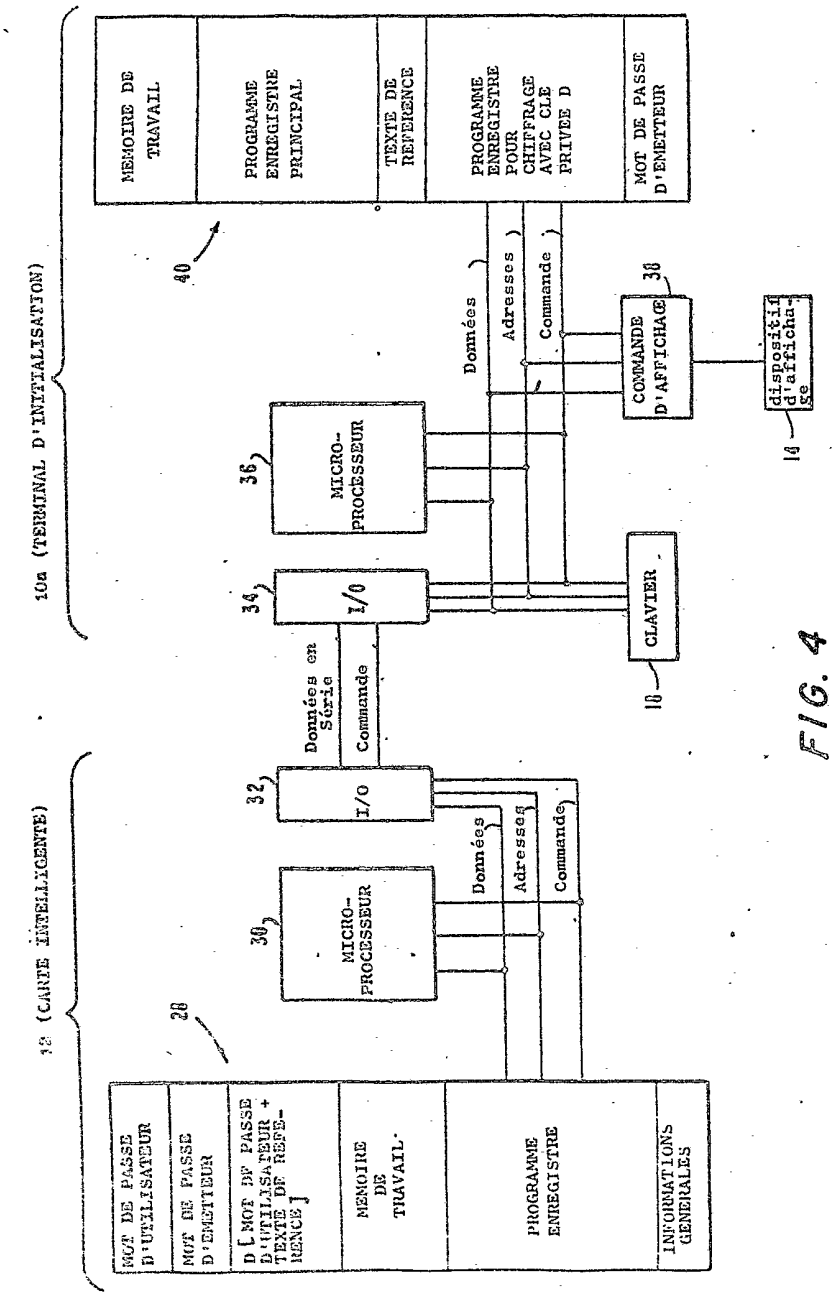

12 (CARTE INTELLIGENTE)
10a (TERMINAL D'INTERVALISATION)
MOT DE PASSE D'UTILISATEUR
MOT DE PASSE D'EMETTEUR
D [MOT DE PASSE D'UTILISATEUR + TEXTE DE REFERENCE]
MEMOIRE DE TRAVAIL
PROGRAMME ENREGISTRE
INFORMATIONS GENERALES
20
MICRO-PROCESSEUR
30
I/O
32
Données en Série
Commande
I/O
34
MICRO-PROCESSEUR
36
Données
Adresses
Commande
CLAVIER
18
COMMANDE D'AFFICHAGE
38
dispositif d'affichage
14
MEMOIRE DE TRAVAIL
PROGRAMME ENREGISTRE PRINCIPAL
TEXTE DE REFERENCE
PROGRAMME ENREGISTRE POUR CHIFFRAGE AVEC CLE PRIVEE D
MOT DE PASSE D'EMETTEUR
40

FIG. 4

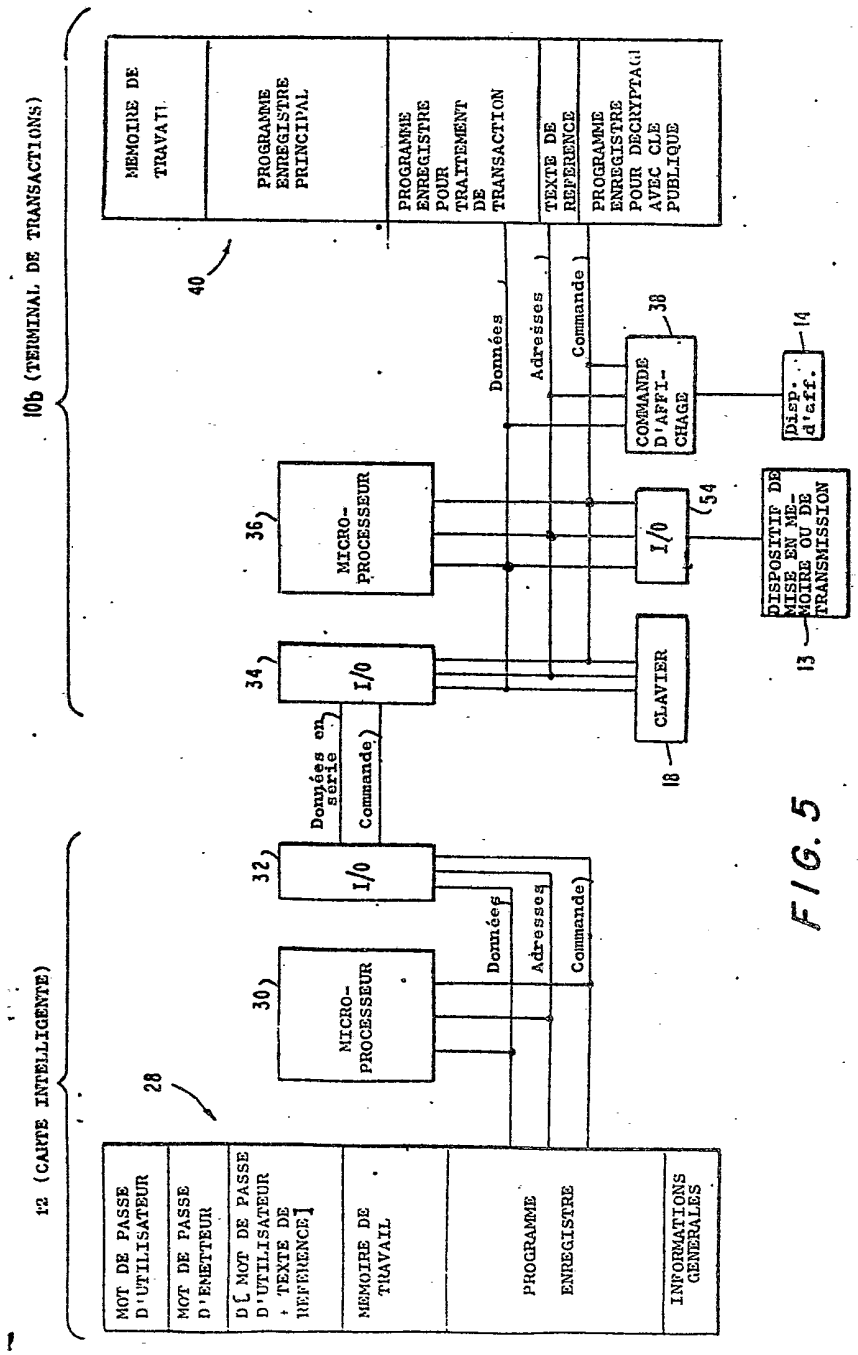

10b (TERMINAL DE TRANSACTIONS)
12 (CARTE INTELLIGENTE)
1
MEMOIRE DE TRAVAIL
PROGRAMME ENREGISTRE PRINCIPAL
PROGRAMME ENREGISTRE POUR TRAITEMENT DE TRANSACTION
TEXTE DE REFERENCE
PROGRAMME ENREGISTRE POUR DECRYPTAGE AVEC CLE PUBLIQUE
40
MOT DE PASSE D'UTILISATEUR
MOT DE PASSE D'EMETTEUR
D(MOT DE PASSE D'UTILISATEUR + TEXTE DE REFERENCE)
MEMOIRE DE TRAVAIL
PROGRAMME ENREGISTRE
INFORMATIONS GENERALES
28
MICRO-PROCESSEUR
30
MICRO-PROCESSEUR
36
I/O
32
I/O
34
Données
Adresses
Commande)
Données en série
Commande)
COMMANDE D'AFFICHAGE
38
Disp. d'aff.
14
I/O
54
CLAVIER
18
DISPOSITIF DE MISE EN MEMOIRE OU DE TRANSMISSION
13

FIG. 5

FIG. 6

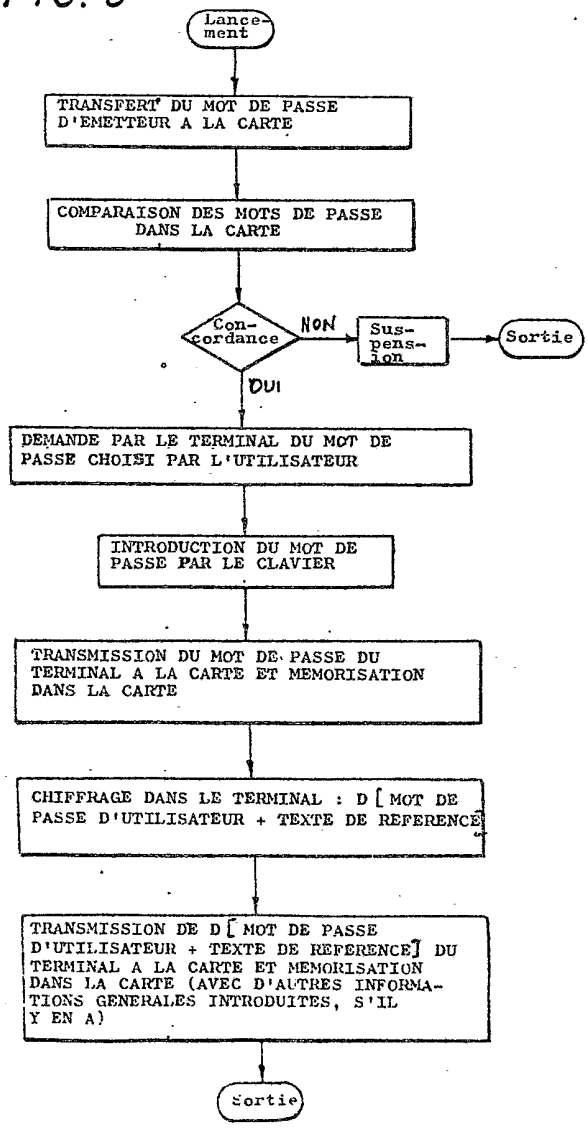
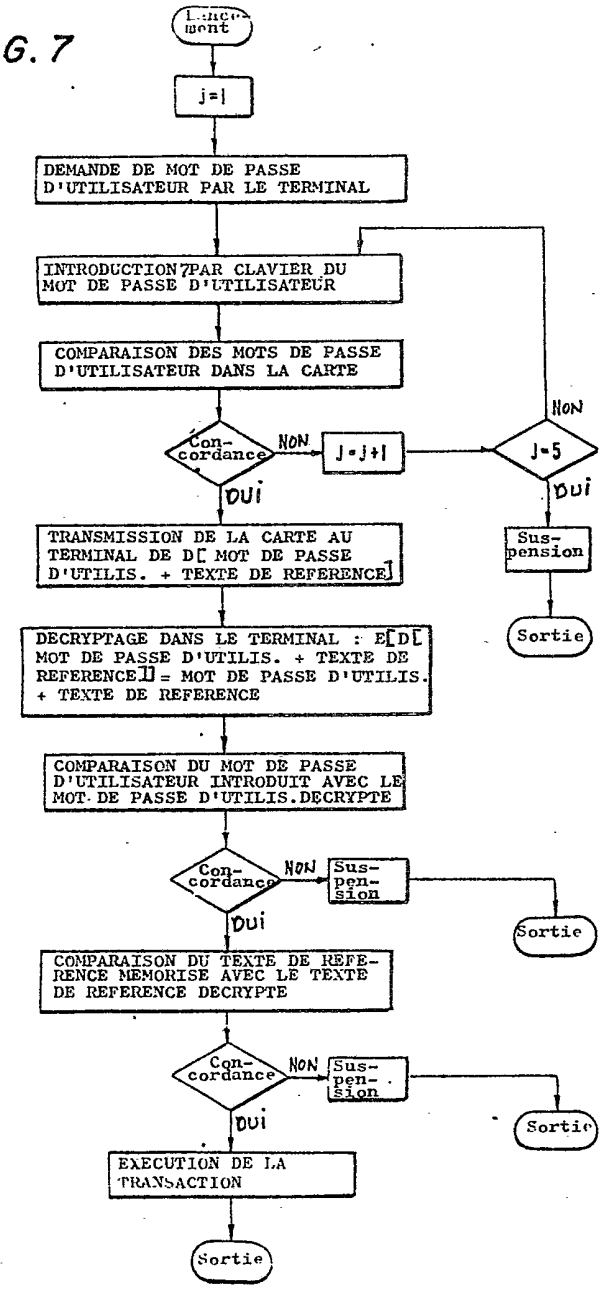

Lance-ment
TRANSFERT DU MOT DE PASSE D'EMETTEUR A LA CARTE
COMPARAISON DES MOTS DE PASSE DANS LA CARTE
Con-cordance
NON
Sus-pens-ion
Sortie
OUI
DEMANDE PAR LE TERMINAL DU MOT DE PASSE CHOISI PAR L'UTILISATEUR
INTRODUCTION DU MOT DE PASSE PAR LE CLAVIER
TRANSMISSION DU MOT DE PASSE DU TERMINAL A LA CARTE ET MEMORISATION DANS LA CARTE
CHIFFRAGE DANS LE TERMINAL : D [MOT DE PASSE D'UTILISATEUR + TEXTE DE REFERENCE]
TRANSMISSION DE D [MOT DE PASSE D'UTILISATEUR + TEXTE DE REFERENCE] DU TERMINAL A LA CARTE ET MEMORISATION DANS LA CARTE (AVEC D'AUTRES INFORMATIONS GENERALES INTRODUITES, S'IL Y EN A)
Sortie

FIG. 7


Lancement
j=1
DEMANDE DE MOT DE PASSE D'UTILISATEUR PAR LE TERMINAL
INTRODUCTION PAR CLAVIER DU MOT DE PASSE D'UTILISATEUR
COMPARAISON DES MOTS DE PASSE D'UTILISATEUR DANS LA CARTE
Concordance
NON
j=j+1
j=5
NON
OUI
OUI
TRANSMISSION DE LA CARTE AU TERMINAL DE D[MOT DE PASSE D'UTILIS. + TEXTE DE REFERENCE]
Suspension
Sortie
DECRYPTAGE DANS LE TERMINAL : E[D[MOT DE PASSE D'UTILIS. + TEXTE DE REFERENCE]] = MOT DE PASSE D'UTILIS. + TEXTE DE REFERENCE
COMPARAISON DU MOT DE PASSE D'UTILISATEUR INTRODUIT AVEC LE MOT DE PASSE D'UTILIS.DECRYPTE
Concordance
NON
Suspension
Sortie
OUI
COMPARAISON DU TEXTE DE REFERENCE MEMORISE AVEC LE TEXTE DE REFERENCE DECRYPTE
Concordance
NON
Suspension
Sortie
OUI
EXECUTION DE LA TRANSACTION
Sortie