



CONFÉDÉRATION SUISSE

OFFICE FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE

⑪ CH 679346 A5

⑤① Int. Cl.⁵: G 09 C 1/00
H 04 L 9/30
H 04 K 1/00

Brevet d'invention délivré pour la Suisse et le Liechtenstein

Traité sur les brevets, du 22 décembre 1978, entre la Suisse et le Liechtenstein

⑫ **FASCICULE DU BREVET** A5

⑳ Numéro de la demande: 4793/88

㉔ Date de dépôt: 23.12.1988

㉓ Priorité(s): 31.12.1987 US 140051

㉒ Brevet délivré le: 31.01.1992

㉑ Fascicule du brevet
publié le: 31.01.1992

㉒ Titulaire(s):
Pitney Bowes Inc. World Headquarters,
Stamford/CT (US)

㉒ Inventeur(s):
Pastor, Jose, Westport/CT (US)

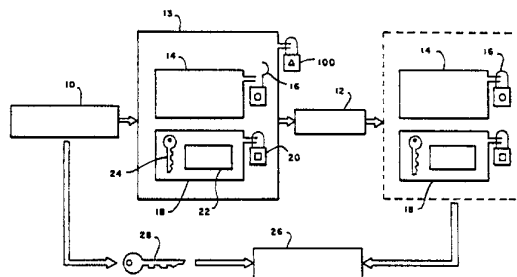
㉒ Mandataire:
E. Blum & Co., Zürich

⑤④ **Dispositif pour l'authentification d'une multitude de documents.**

⑤⑦ Un dispositif pour l'authentification d'une multitude de documents comprend une source d'authentification (10), un moyen (13) pour fournir un message à l'utilisateur, un moyen (14, 41) pour générer des variables et des valeurs, un moyen (34) pour récupérer le message et un moyen (18) pour fournir la clé de déchiffrement.

L'utilisateur reçoit de la source (10) une première clé de chiffrement (E2) pour chiffrer un document. Parallèlement, le moyen (13) fournit le message qui est chiffré pour une seconde clé de chiffrement (E1) et qui comporte également la clé de déchiffrement (24, D2) pour la première clé de chiffrement. Le moyen (34) pour récupérer le message se trouve à un service d'authentification qui obtient la clé (E1) par le moyen (18) pour déchiffrer le message, qui peut ainsi obtenir la clé de déchiffrement (24, D2) pour déchiffrer le document.

Le dispositif peut être utilisé par un expéditeur de courrier, le service d'authentification peut être la poste qui vérifie l'impression chiffrée d'affranchissement.



Description

La présente invention concerne l'authentification d'une multitude de documents selon le préambule de la revendication 1.

L'une des tâches historiques entreprises par de nombreuses personnes et organisations a été d'assurer l'authenticité des documents. L'importance qu'il y a à prouver réellement l'authenticité d'un document va de la simple identification d'une signature à la vérification des informations militaires et/ou politiques. En outre, toutes les fois qu'on essaie de démontrer l'authenticité d'un document, il y a généralement au moins une partie qui tente de la contrefaire. Par conséquent, il y a eu, et il y aura probablement encore, un combat pour pouvoir authentifier des documents.

Au cours des ans, les progrès technologiques ont donné une nouvelle signification au mot «document».

Actuellement, un document peut être, par exemple, un récépissé produit électroniquement dans une machine bancaire ou un enregistrement numérisé sur un disque optique. Dans le cadre de la présente demande de brevet, on interprétera par conséquent le mot «document» comme incorporant une information placée sur un support quelconque dont, mais sans que cela soit limitatif, les disques magnétiques, les disques optiques ou le papier.

Une autre tâche similaire qui a une histoire aussi colorée que l'authentification des documents est la communication sûre de l'information entre deux parties. Une telle communication de l'information comprend généralement l'utilisation des techniques de chiffrement/déchiffrement. D'une façon similaire à la contrefaçon mentionnée ci-dessus, il y a en général au moins une partie qui est intéressée soit à voler l'information communiquée qui a été chiffrée, soit à fournir une fausse information dans un format chiffré de sorte que son destinataire est désinformé, soit à procéder aux deux. Par conséquent, au cours des années, on a mis au point divers plans de chiffrement/déchiffrement dont on pensait, au moins pendant une certaine période, qu'ils étaient sûrs pour découvrir que cette sécurité avait été compromise. Là encore, les progrès technologiques ont considérablement changé le domaine de la cryptographie. Par exemple, avec les ordinateurs modernes on peut enfreindre les techniques cryptographiques dans un laps de temps relativement court, grâce, principalement, à la vitesse à laquelle les ordinateurs exécutent les opérations mathématiques.

On connaît une technique cryptographique actuellement sûre sous la forme du système cryptographique à clés publiques. Une forme particulière de ce système est décrite et discutée dans un article intitulé «A Method for Obtaining Digital Signatures and Public Key Cryptosystems» de R.L. Rivest, A. Shamir and L. Adleman, Volume 21 #2, février 1978, Communications of ACM pages 120-126. (Procédé pour obtenir des signatures numériques et des cryptosystèmes à clés publiques). Ce système particulier est fréquemment appelé cryptosystème public à clés publiques RSA.

Les techniques à clés publiques, comme cela est

souligné dans l'article intitulé «Public Key Cryptography» de John Smith, dans l'édition de janvier 1983 de Byte Magazine, pages 189-218 (Cryptographie à clés publiques) comportent généralement deux types différents de clés: les clés de chiffrement et les clés de déchiffrement. Ces clés présentent les propriétés suivantes: a) il est possible de calculer une paire de clés comportant une clé de chiffrement et une clé de déchiffrement; b) pour chaque paire, la clé de déchiffrement n'est pas la même que la clé de chiffrement, et c) il n'est pas possible de calculer la clé de déchiffrement même à partir de la connaissance de la clé de chiffrement. De plus, dans un tel cryptosystème, les clés de chiffrement et de déchiffrement sont fonctionnellement réversibles, c'est-à-dire que si on utilise une clé pour le chiffrement, on peut employer l'autre clé pour déchiffrer ce qui a été chiffré.

Comme on le sait, l'expression «clé publique» provient du fait que la clé de chiffrement de chaque partie est disponible, c'est-à-dire publique, pour toutes les parties souscrivant au réseau particulier à clés publiques impliqué. Par exemple, dans leur utilisation générale, les systèmes cryptographiques à clés publiques sont conçus pour une communication directe entre deux parties qui souscrivent, chaque partie ayant une clé de déchiffrement non publiée et une clé de chiffrement publiée.

Le système cryptographique à clés publiques a également trouvé une utilisation dans la fourniture d'une identification précise de la source d'un document. Comme cela est discuté dans les pages 217-218 de l'article de Smith, un expéditeur peut effectivement signer un message en le chiffrant en premier lieu, ou en authentifiant une partie, par exemple, son nom en utilisant sa clé privée de déchiffrement et en chiffrant en second lieu le message avec la clé publique de chiffrement du tiers de destination. Cela se traduit par une partie du message que seul l'expéditeur peut avoir créée et que seul le destinataire peut lire. Par conséquent, une communication entre deux parties peut, dans la mesure où les systèmes cryptographiques à clés publiques sont de sécurité, être mise en œuvre d'une façon telle qu'on puisse assurer l'authenticité d'un document.

Néanmoins, il reste de nombreux cas où il y a un besoin, ou un désir, pour qu'un tiers authentifie un document concernant deux autres parties, ou transmis entre deux parties. Un exemple d'une telle situation est le cas où il est demandé à une première partie, ou simplement désiré, de prouver ou de faire la démonstration de l'authenticité d'un document particulier destiné à une seconde partie. Dans une telle situation, il pourrait être des plus bénéfiques qu'une troisième partie puisse fournir un moyen pour authentifier le document. Une situation particulière pourrait exister dans le cas où un différend sur l'authenticité d'un document serait soulevé entre deux parties et qu'une troisième partie impartiale serait choisie pour résoudre le problème à la satisfaction des deux premières. Une telle situation pourrait se produire lorsque, conformément à un accord entre les deux parties, l'une d'elles devait conserver certains enregistrements de façon que la se-

conde partie puisse les réexaminer afin d'assurer leur conformité à l'accord. Dans une telle situation, il serait des plus bénéfiques qu'une troisième partie soit disponible pour faire la démonstration de la précision/imprécision des enregistrements pour le compte de la seconde partie.

Une autre situation encore plus largement rencontrée, représentative de l'authentification d'un document par une troisième partie, est le domaine de traitement du courrier dans lequel un expéditeur doit prouver au service postal l'authenticité du fait qu'il a payé l'affranchissement d'une expédition particulière. Il est courant que les services postaux américains dits United States Postal Service (USPS) acceptent les signes qui ont été appliqués sur une enveloppe par un expéditeur comme représentatif du fait que l'affranchissement nécessaire à l'acheminement de l'enveloppe a été réglé. De fait, dans de nombreux cas, le signe est appliqué, par exemple, par un appareil d'affranchissement en location et le constructeur de cet appareil donne l'assurance au service USPS que lorsque l'appareil d'affranchissement est mis en service pour imprimer le signe, l'affranchissement ou valeur monétaire de l'expédition a été réglé. Actuellement, les appareils d'affranchissement appliquent des signes sur une enveloppe via un moyen mécanique d'impression tel qu'un tambour sur lequel on a gravé des signes, ou via une impression par platine sur une enveloppe. Cependant, grâce principalement aux progrès technologiques, l'utilisation de plus en plus grande de l'impression sans contact a rendu souhaitable de faire appel à de telles techniques dans les systèmes de traitement du courrier. Cependant, l'utilisation des techniques d'impression sans contact peut actuellement conduire à une comptabilisation imprécise sauf à fournir des techniques sûres.

Une technique sûre serait l'emploi des techniques courantes de chiffage dans lesquelles un expéditeur aurait une clé cryptographique qui lui permettrait de chiffrer l'information et de placer cette information sur l'enveloppe. Les services USPS, par exemple, pourraient alors, en utilisant une clé cryptographique identique, déchiffrer l'information présente sur l'enveloppe et avoir l'assurance que l'affranchissement a été réglé. Un inconvénient majeur d'un tel système serait, naturellement, qu'il existe des milliers d'expéditeurs et que par conséquent les services USPS devraient conserver une très grande base de données des clés cryptographiques afin de permettre le déchiffrement de toutes les clés de chiffage différentes réparties entre les divers expéditeurs.

En variante, on peut éviter d'avoir à faire appel à une base de données assez massive en utilisant un système tel que celui décrit dans la demande de brevet des Etats-Unis d'Amérique n° 136 251, qu'on incorporera ici à titre de référence.

Le système décrit dans cette demande de brevet comprend la mise en œuvre d'un système cryptographique à clés publiques pour trois parties. Dans ce système, dans la mesure où il concerne un système de traitement du courrier, un expéditeur est, par essence, muni de deux informations. Une information permet à l'expéditeur de chiffrer les renseigne-

ments concernant une expédition. L'autre information permet au service postal non seulement de déchiffrer l'information cryptée par l'expéditeur, mais aussi d'authentifier chaque document. Ainsi, dans un mode de réalisation, chaque enveloppe comprend une information variable sur l'utilisateur et une information spécifique (fixe) sur l'utilisateur. Cependant, afin d'assurer la sécurité, chacune des deux informations comprendra typiquement entre cent et deux cents chiffres. Ainsi, cela peut être, en soi, un inconvénient considérable pour la vitesse et l'efficacité du système.

Par conséquent, il serait extrêmement souhaitable de disposer d'un système permettant d'acheminer de manière fiable une information afin d'authentifier une multitude de documents en général, et d'acheminer cette information de façon que l'information d'authentification puisse n'être déterminée qu'à partir d'une multitude d'articles individuels.

En conséquence, la présente invention a pour objet un système pour acheminer des informations afin de permettre une authentification fiable d'une multitude de documents, qui surmonte sensiblement les inconvénients venant d'être exposés.

Cet objet est réalisé, au moins en partie, par un dispositif comme défini dans la revendication 1.

La présente invention sera bien comprise lors de la description suivante faite en liaison avec les dessins ci-joints dans lesquels:

La fig. 1 est un schéma conceptuel d'un système selon les principes de la présente invention;

La fig. 2 est un schéma sous forme de blocs d'un système selon la présente invention; et

La fig. 3 est un organigramme de la circulation de l'information dans le système représenté en fig. 2.

Comme on l'a discuté ci-dessus, un tiers ou troisième partie neutre représentée dans ses grandes lignes par la référence 10, en tant que source d'authentification, en fig. 1, établit un certain nombre de paires de clés publiques de chiffage/déchiffage.

Lorsqu'un utilisateur 12 souhaite faire appel aux services offerts par la source d'authentification 10, une paire de clés est sélectionnée et affectée à l'utilisateur 12 lorsqu'il rejoint le service. Plus précisément, l'utilisateur 12 reçoit la clé E_2 de la paire E_2D_2 . L'utilisateur 12 reçoit alors de préférence une boîte 13 contenant des boîtes 14 et 18. Chaque boîte 13 est fermée avec un verrou 100. Le verrou 100 a été fermé avec la clé D_2 , qui ne peut être déverrouillée qu'avec la clé E_2 . L'utilisateur 12 déverrouille la boîte 100 avec la clé E_2 et ouvre la boîte 13 pour trouver les première et seconde boîtes 14 et 18. En variante, l'utilisateur 12 peut ne recevoir que la première boîte 14 et la seconde boîte 18. Quoi qu'il en soit, la première boîte 14 comporte un verrou d'ouverture 16, le verrou 16 représentant les opérations de chiffage/déchiffage avec la paire affectée de clés E_2D_2 . De plus, l'utilisateur 12 reçoit une seconde boîte 18 qui est fermée par le verrou 20, la boîte fermée 18 l'étant via la clé de chiffage E_1 d'une paire non affectée de clés, E_1D_1 , la clé de chiffage non affectée E_1 étant maintenue en se-

cret absolu par la source d'authentification 10. La seconde boîte 18 contient, essentiellement, un certificat 22 représentatif de la source d'authentification 10 et de la clé de déchiffrement (D_2) 24 de la paire affectée de clés pour ouvrir la boîte fermée 14 fournie à l'utilisateur 12 à l'état déverrouillé. L'utilisateur 12 place alors l'information, ou la documentation, qui est unique pour lui à l'intérieur de la première boîte déverrouillée 14 et ferme le verrou 16 avec la clé E_2 . L'utilisateur 12, dans ce type de concept, confiera alors les deux boîtes verrouillées 14 et 18 au service d'authentification 26. Le service 26 est muni de la clé de déchiffrement D_1 , 28, par la source d'authentification 10. Cette clé D_1 est commune à tous les verrous de toutes les secondes boîtes 18 créées par la source d'authentification 10. La clé de chiffrement correspondante E_1 de la paire non affectée de clés, comme on l'a mentionné ci-dessus, est maintenue en secret par la source d'authentification 10.

Par conséquent, pour authentifier le document fourni par l'utilisateur 12, le service d'authentification 26 déverrouille simplement, c'est-à-dire déchiffre, la seconde boîte verrouillée 18 et reconnaît immédiatement le certificat d'authenticité 22 provenant de la source d'authentification 10. Dans le cas où le service d'authentification 26 souhaite alors s'assurer, à titre de vérification ou pour une autre raison, de l'information de l'utilisateur, la clé de déchiffrement 24 de la paire affectée de clés est maintenant à sa disposition pour déverrouiller la première boîte 14 qui a été ouverte lors de sa fourniture à l'utilisateur 12.

Il en résulte qu'un nombre quelconque d'utilisateurs 12 peuvent demander un nombre quelconque de boîtes déverrouillées 14 dans lesquelles ils souhaitent placer une information pour authentification par le service d'authentification 26. Cependant, le service d'authentification 26 a besoin de ne conserver que la seule clé de déchiffrement 28 correspondant à tous les verrous de toutes les secondes boîtes verrouillées 18 fournies aux utilisateurs 12. Ainsi, chaque seconde boîte 18, comme on l'a indiqué ci-dessus, contient le certificat d'authenticité 22 ainsi que la clé de déchiffrement 24 de la paire affectée de clés afin de déverrouiller la première boîte 14 contenant l'information de l'utilisateur.

Ainsi, il n'y a aucune clé publique dans ce système de cryptographie à «clés publiques», et bien que le système soit semblable à un système secret à clés, par exemple, au système DES, la nécessité de faire appel au service d'authentification 26 pour maintenir une base de données massive est éliminée car tous les verrous de toutes les secondes boîtes 18 données à l'origine aux utilisateurs 12 peuvent être déverrouillés par la seule clé de déchiffrement 28 de la paire non affectée de clés fournie au service d'authentification 26 par la source d'authentification 10. En outre, à moins qu'il y ait un besoin prioritaire, le simple déverrouillage des secondes boîtes verrouillées 18 fournies aux utilisateurs 12 par le service d'authentification 10 est suffisant pour faire la démonstration que l'utilisateur 12 fonctionne à l'intérieur du système car, pour avoir accès à la seconde boîte 18, l'utilisateur 12 a dû, lors

de la réception de la boîte 13, déverrouiller le verrou 100 avec la clé E_2 que ne possède que cet utilisateur 12. Par conséquent, l'information de l'utilisateur peut, de fait, être maintenue en sécurité et en secret complet. En outre, il peut y avoir néanmoins accès à l'information réelle, dans le cas où cela s'avérerait nécessaire, par l'emploi de la clé de déchiffrement 24 de la paire affectée de clés accompagnant le certificat 22 d'authenticité.

Comme on le décrit plus pleinement ci-après, dans un mode de réalisation de l'invention, le verrou ouvert 16 accompagnant la première boîte 14 sera fermé avec la clé de chiffrement de la paire de clés publiques de chiffrement/déchiffrement, E_2D_2 , affectée à l'utilisateur 12. La clé 24 se trouvant à l'intérieur de la seconde boîte verrouillée 18 sera la clé de déchiffrement D_2 de la paire de clés publiques de chiffrement/déchiffrement E_2D_2 affectée à l'utilisateur 12. La seconde boîte 18 est verrouillée en chiffrant le certificat d'authenticité 22 et la clé de déchiffrement 24 pour la première boîte 14 avec la clé de chiffrement E_1 de la paire de clés chiffrées, non affectées, représentant ainsi, par exemple, une chaîne de chiffres. La clé 28 fournie au service d'authentification 26 sera la clé de déchiffrement D_1 de la paire non affectée de clés maintenue en sécurité par la source d'authentification. Etant donné que, au moins en ce qui concerne un système cryptographique RSA à clés publiques, la sécurité augmente comme le produit des nombres premiers servant de base pour la génération des paires de clés, chaque document du présent système peut comprendre deux ensembles de chiffres, chaque ensemble ayant au moins cent chiffres. Généralement, un ensemble de chiffres représentera l'information chiffrée de l'utilisateur qui variera généralement pour chaque document. L'autre ensemble de chiffres représentera la seconde boîte verrouillée 18 et sera généralement invariable pour chaque document produit par l'utilisateur 12 d'une paire de clés affectée.

Dans le système décrit ci-dessus, comme avec n'importe quel cryptosystème du type à clés publiques, chaque ensemble de chiffre devra, afin d'améliorer la sécurité, comprendre éventuellement un à deux cent chiffres. Ce nombre de chiffres qu'il faut pour chaque document peut être réduit lorsqu'un seul utilisateur 12 délivre une multitude de documents au service d'authentification 26.

A titre d'exemple seulement, dans un mode de réalisation, un utilisateur particulier 12 est un expéditeur qui délivre son courrier au service postal (service d'authentification 26). Dans le but de réduire le nombre de caractères de l'ensemble invariable imprimé sur chaque enveloppe, on choisit un nombre N . Le nombre N représente le nombre d'enveloppes qui doivent être accumulées par le service postal pour reconstruire l'ensemble invariable de caractères. L'ensemble invariable de caractères est alors divisé en N blocs de caractères. Chaque valeur de N est utilisée comme coefficient «a» dans, par exemple un polynôme ayant la forme suivante:

$$f(x_i) = a_1x_i + a_2(x_i)^2 \dots a_n(x_i)^n$$

Chaque coefficient est inférieur à un nombre premier «P» et toutes les équations sont exécutées en modulus P d'une façon semblable à une technique discutée par Adi Shamir dans «How to Share a Secret», in Communication of the ACM, Novembre 1979 Vol. 22; n° 11; pages 612-613» (Comment partager un secret). Cependant, Shamir utilise de façon différente la totalité du secret comme l'un des coefficients. Par conséquent, le nombre «P» est plus long que le secret. En conséquence, comme tous les opérateurs sont à un Modulus P, toutes les valeurs peuvent être aussi longues que «P». Il en résulte que la technique de Shamir ne réduira pas la longueur de l'information imprimée.

L'utilisateur 12 produit alors aléatoirement, les valeurs de x, résoud le polynôme et imprime x_i , $f(x_i)$ sur chaque enveloppe. En conséquence, connaissant le degré du polynôme, c'est-à-dire l'exposant le plus élevé, soit à partir de la source d'authentification 10 soit à partir de l'utilisateur 12, le service d'authentification 26 peut accumuler «n» plis du courrier et résoudre le jeu des équations pour reconstruire l'ensemble invariable. Ensuite, l'ensemble invariable de caractères peut être déchiffré pour obtenir le certificat d'authenticité 22.

Dans une variante de réalisation, la source d'authentification 10 peut fournir à l'utilisateur 12 l'ensemble invariable de caractères déjà sous la forme des coefficients a_i .

Un système 29 pour authentifier les documents de façon fiable est représenté en fig. 2 dans laquelle la source d'authentification 30 comprend un générateur 32 de paires de clés publiques, un ensemble de traitement 34, une mémoire rémanente 36, une mémoire 38 fonctionnant en temps réel et une interface de communication 40 et, dans un mode de réalisation, un générateur de polynômes 41. De préférence, le générateur 32 de paires de clés publiques comprend un générateur de clés publiques de chiffrement/déchiffrement dit RSA qui peut incorporer une puce RSA de chiffrement/déchiffrement qu'on peut se procurer, par exemple, auprès de la société dite CYLINK de Sunnyvale, Californie.

L'ensemble de traitement 34 peut être un processeur ou ordinateur à usage général, destiné à manipuler l'information en conformité avec la fonction désirée.

De préférence, la mémoire rémanente 36 peut être un disque magnétique, une bande magnétique, etc., à laquelle l'ensemble de traitement 34 peut accéder. La mémoire 38 à fonctionnement en temps réel peut être, entre autres, une mémoire à accès direct à semi-conducteur ou un disque souple.

Dans un mode de réalisation spécifique, l'interface de communication 40 peut comporter une carte enfichable à circuits imprimés de télécommunication. L'interface 40 est de préférence connectée à l'expéditeur 42 et au fournisseur 44 de services postaux.

L'expéditeur 42 comprend un module de chiffrement 46 destiné à chiffrer l'information via un système de cryptographie à clés publiques RSA. De plus,

l'expéditeur 42 comprend une mémoire rémanente 48 dans laquelle est stockée la clé de la paire affectée de clés publiques et un générateur de nombres au hasard. Une interface 50 de communication compatible est prévue pour permettre des communications à distance avec la source d'authentification 30 et un processeur 52 est incorporé pour permettre la manipulation de l'information chiffrée qui est reçue, ayant été entrée par l'expéditeur 42 via le dispositif d'entrée 54.

A la suite de la préparation du courrier, l'expéditeur 42 le délivre au service d'authentification 44 qui, par exemple, peut être un bureau de poste local. Dans ce mode de réalisation particulier, le service 44 comprend un dispositif de déchiffrement 56, incorporant un module de déchiffrement ayant une mémoire volatile associée, dans laquelle est stockée la clé de déchiffrement de la paire non affectée de clés publiques pour ce système particulier. La clé de déchiffrement de la paire non affectée peut, dans un mode de réalisation, être la même pour chaque lieu 44 de service. Cependant, le cas échéant, la clé de déchiffrement des lieux 44 de service pourrait dépendre, par exemple, de sa situation géographique mais néanmoins, de manière uniforme dans toute une région géographique particulière. Cependant, aucun des lieux 44 de service n'a besoin de conserver une base de données des clés. De plus, le service d'authentification 44 comprend un moyen 58 d'entrée de données qui peut être, par exemple, un clavier, un lecteur optique ou tout autre moyen pour transférer l'information de la face, par exemple, d'une enveloppe ou d'un manifeste à un processeur 60 se trouvant à l'intérieur du dispositif de déchiffrement 56. Le processeur 60 résout aussi initialement le polynôme pour fournir au dispositif de déchiffrement 56 l'ensemble invariable des caractères à déchiffrer. De préférence, le dispositif de déchiffrement 56 comprend en outre un dispositif de visualisation 62 pour fournir une indication rapide soit visuelle soit audio, de l'authenticité de l'information présente sur l'enveloppe qu'on vérifie. En outre, dans un mode de réalisation particulier, le dispositif de déchiffrement 56 est destiné à communiquer via une interface de communication 64 avec la source d'authentification 30.

La circulation de l'information dans le système typique 29 représenté en fig. 2 est décrite plus clairement en fig. 3. Dans cette figure, une table 32 de paires de clés publiques de chiffrement/déchiffrement est représentée telle qu'elle serait produite par le générateur de clé 32 de la source d'authentification 30. Comme cela est représenté, une paire de clés est affectée, à partir de la table, à un utilisateur 42 sur demande ou lors d'un changement régulier de clé. De préférence, de manière à améliorer la vitesse d'authentification, un message M en texte en clair est chiffré en utilisant la clé de chiffrement non affectée qui est conservée en sécurité par la source d'authentification. En plus du message, la clé affectée de déchiffrement qui correspond à la clé de chiffrement affectée, fournie à l'utilisateur 42, est également chiffrée en utilisant la clé de chiffrement non affectée. En outre, dans un mode de réalisation

tion, un polynôme $f(x_i)$ est produit pour chaque paire de clés devant être affectées à des utilisateurs 12. Ce polynôme est acheminé jusqu'à l'utilisateur 12.

En fonctionnement, l'utilisateur 42 peut alors entrer l'information, par exemple, une information d'expédition et en recevoir un message chiffré de sortie. Le message chiffré de sortie est transmis via une sortie 66 pour être imprimé, dans un mode de réalisation, sur une enveloppe, ou autre document d'expédition, par un moyen quelconque mis à la disposition de l'expéditeur, par exemple par une imprimante sans contact 68. De plus, la valeur calculée de $f(x_i)$, x_i de l'ensemble invariable de caractères est également appliquée aux enveloppes.

Le courrier est ensuite présenté au service postal 44 pour paiement, traitement, expédition etc. A ce moment là, le service postal 44 peut choisir d'authentifier un ou plusieurs des plis de courrier. De manière à exécuter l'authentification, «n» enveloppes différentes sont accumulées et la valeur x_i de la fonction $f(x_i)$ de chacune est entrée dans le processeur. Le processeur résout les polynômes et entre l'ensemble invariable de caractères dans le dispositif de déchiffrement 56, à la suite de quoi, il est déchiffré par l'utilisation de la clé de déchiffrement de la paire de clés publiques non affectées qui est produite par la source d'authentification 30 et correspondant à la clé de chiffrement qui est maintenue au secret. Lors du déchiffrement, l'authenticité est déterminée, c'est-à-dire que le pli de courrier ou le document est correct et conforme aux règles établies par la source d'authenticité 30. En variante, le dispositif de visualisation 62 peut indiquer l'authenticité même si le document spécifique ne provient pas de l'utilisateur 12. L'identité de l'utilisateur 12 peut, cependant, être assurée si la source d'authentification 10 chiffre le message (M) et la clé affectée de déchiffrement correspondant à la clé affectée de chiffrement utilisant la clé affectée de déchiffrement. Cela est possible car la fonction de la clé, c'est-à-dire la fonction de chiffrement ou de déchiffrement, est réversible. Par conséquent, pour que l'utilisateur 12 obtienne l'information nécessaire devant être placée sur un document d'expédition, c'est-à-dire le message chiffré (M) et la clé affectée de déchiffrement, il doit d'abord déchiffrer, en utilisant la clé affectée de chiffrement, l'information donnée par la source d'authentification 10. Ainsi, si le service postal 44 déchiffre l'information présente sur le document d'expédition et reconnaît le message (M), il y a preuve de l'identité de l'utilisateur 12.

Dans une variante de réalisation, dans laquelle la source d'authentification 10 et l'utilisateur 12 partagent une seule clé identique, l'utilisateur 12 peut alors imprimer une partie tronquée de l'information invariable chiffrée. Le service d'authentification 26 peut, le cas échéant, reconstruire la partie tronquée en chiffrant l'information invariable en texte clair provenant de l'enveloppe.

Avantageusement, en plus de la fourniture d'un système fiable d'authentification d'une multitude de documents, le système 29 décrit ici est avantageux car il faut une information moins importante sur

chaque enveloppe. En outre, de nouvelles paires de clés peuvent être affectées aux expéditeurs 42 sans que la clé du bureau de poste soit mise à jour. Cela présente un intérêt particulier car la synchronisation des clés, lorsque les clés sont fréquemment modifiées, est difficile à maintenir dans de nombreux systèmes. Par exemple, dans les systèmes où chaque clé n'est utilisée qu'une fois et des clés sont employées dans une séquence pré-disposée, il y a le problème que des messages peuvent ne pas être reçus dans l'ordre. Ainsi, si deux messages sont transposés, la clé de destination peut ne pas correspondre à la clé-source. Dans le présent système 29, cela n'est pas un problème car le déchiffrement nécessaire est, dans le plan macroscopique, commun à tous les messages et dans le plan spécifique de l'utilisateur, l'information concernant la clé de déchiffrement accompagne le message lui-même et par conséquent, ne peut éventuellement être désordonnée. De fait, l'expéditeur 42 pourrait utiliser n'importe quel nombre de clés affectées dans une séquence aléatoire, réutiliser les clés et ne pas employer de clés du tout sans que cela affecte le service d'authentification 44.

Ainsi, dans un système 29 de traitement au courrier dans lequel un nombre important de clés sont utilisées pour un nombre important d'expéditeurs 42, un tel système présente des avantages notables. Par exemple, le bureau de poste n'a pas besoin de conserver une base de données; de fait, il doit conserver seulement une seule clé de déchiffrement, d'où la réduction des problèmes de sécurité ainsi que des problèmes concernant les bases de données. De plus, l'expéditeur 42 peut se voir affecter une nouvelle clé à tout instant sans le risque que le bureau de poste ne soit pas mis à jour au moment où arrive le message ainsi chiffré. Ainsi un certain nombre de clés peuvent être utilisées pour un nombre quelconque de transmissions différentes ou, de fait, identiques tout en ayant l'assurance complète que le bureau de poste peut décoder chaque message. En outre, les problèmes ordinaires de sécurité concernant toute forme de système cryptographique sont compartimentés. Par exemple, la perte de sécurité d'une liaison du système 29 ne détruit pas l'intégrité du système. De plus, comme avantage pour l'expéditeur, alors que dans certains types d'expédition il est nécessaire de déposer son courrier dans un bureau de poste désigné, cette exigence peut être éliminée. L'élimination de cette exigence provient du fait que chaque bureau de poste peut être muni de la même clé de déchiffrement, et qu'en conséquence, un expéditeur 42 peut déposer son courrier dans n'importe quel bureau de poste et savoir que le bureau recevant ce courrier peut néanmoins déterminer l'authenticité de l'information qu'il porte.

On remarquera que l'expéditeur 42 peut fournir l'information sur une enveloppe en utilisant un appareil d'affranchissement au lieu d'un mécanisme d'impression sans contact. Dans un tel mode de réalisation, l'actionnement de l'imprimante associée à l'appareil d'affranchissement dépendra de la réception de l'information correcte en provenance de l'expéditeur 42. Une telle information sera acheminée,

comme preuve du paiement, avec le courrier jusqu'au bureau de poste.

La présente invention n'est pas limitée aux exemples de réalisation qui viennent d'être décrits, elle est au contraire susceptible de modifications et de variantes qui apparaîtront à l'homme de l'art.

Revendications

1. Dispositif pour l'authentification d'une multitude de documents, caractérisé en ce qu'il comprend:

- une source d'authentification (10), cette source comportant un moyen pour fournir à un utilisateur (12) une première clé publique de chiffage (E2);
- un moyen (13) associé à la source (10), pour fournir un message d'authentification (22) à l'utilisateur (12) sous forme d'un coefficient (a) d'un polynôme, ce message (22) étant chiffré par une seconde clé publique de chiffage (E1) et comportant la clé de déchiffage (24, D2) pour la première clé;
- un moyen (14, 41) associé à l'utilisateur (12) pour générer des variables et des valeurs pour le polynôme et appliquer des variables et valeurs différentes à chaque document de la multitude de documents;
- un moyen (34) associé à un service d'authentification (26), pour récupérer le message d'authentification (a) auprès d'une multitude de variables et valeurs différentes parmi les variables et valeurs; et
- un moyen (18), associé à la source (10), pour fournir la clé de déchiffage (28, D1) correspondant à la seconde clé de chiffage (E1) au service d'authentification (26) de façon que le message d'authentification (22) puisse être déchiffré.

2. Dispositif selon la revendication 1, caractérisé en ce qu'il est apte à fournir un message d'authentification (22) qui est chiffré en utilisant la clé de déchiffage (D2) pour la première clé de chiffage (E2).

3. Dispositif selon la revendication 1, caractérisé en ce qu'il est apte à fournir un message d'authentification (22) qui comprend en outre un message de certification qui, lorsque le message est déchiffré, fournit une vérification du texte en clair que le message d'authentification a son origine à la source d'authentification (10).

4. Dispositif selon la revendication 3, caractérisé en ce qu'il est apte à être utilisé par un utilisateur qui est un expéditeur (12) d'une multitude de plis de courrier et la première clé de chiffage (E2) sert à chiffrer une information relative au courrier.

5. Dispositif selon la revendication 4, caractérisé en ce qu'il est apte à appliquer l'information relative au courrier à chaque document d'une multitude de documents du courrier et chacune des variables et des valeurs correspondantes est appliquée à des documents différents de la multitude de documents.

6. Dispositif selon la revendication 1, caractérisé en ce que la première clé de chiffage (E2) et la clé de déchiffage (D2) pour la première clé sont identiques.

7. Dispositif selon la revendication 6, caractérisé en ce qu'il est apte à appliquer l'information relative au courrier qui figure sur l'enveloppe en forme

d'une partie tronquée de l'information chiffrée relative au courrier.

8. Dispositif selon la revendication 1, caractérisé en ce que le moyen de génération (41) comporte un générateur de nombres au hasard qui lui est associé.

9. Dispositif selon la revendication 1, caractérisé en ce qu'il comprend en outre un moyen (28) pour fournir au service d'authentification (26) l'ordre du polynôme.

10. Dispositif selon la revendication 9, caractérisé en ce que le moyen (13) de fourniture du polynôme est associé à la source d'authentification (10).

11. Dispositif selon la revendication 9, caractérisé en ce que le moyen (13) fournissant le polynôme est associé à l'utilisateur.

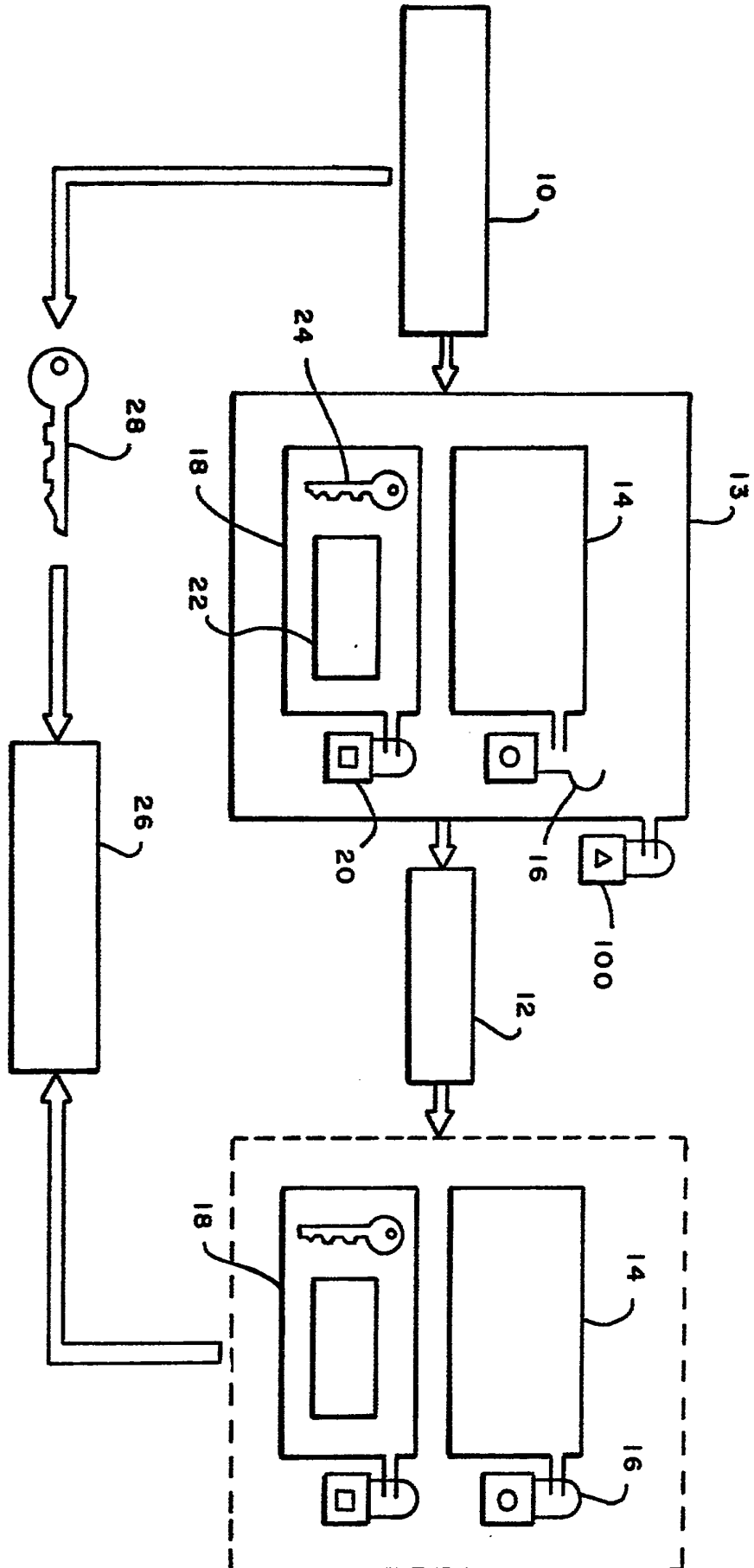


FIG. 1

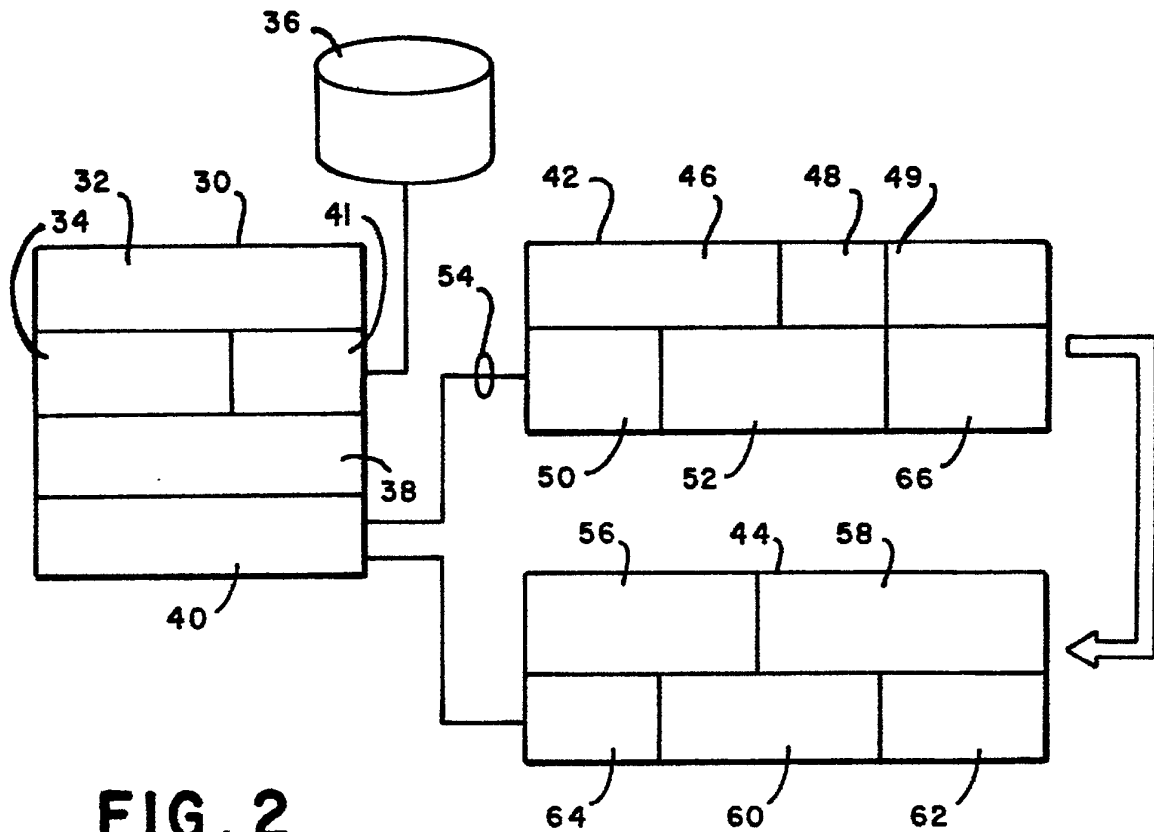


FIG. 2

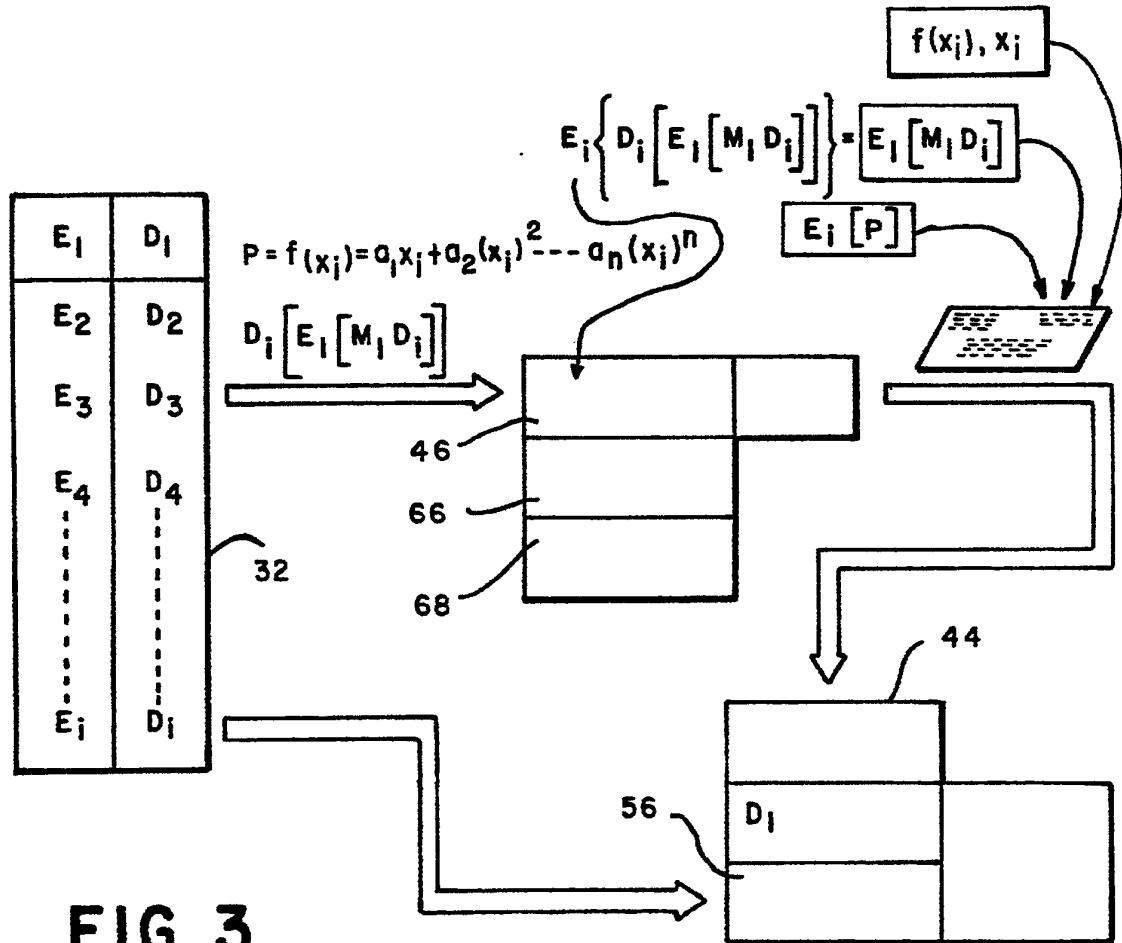


FIG. 3