

THESIS / THÈSE

MASTER EN SCIENCES INFORMATIQUES

La transmission des résultats d'analyses médicales en médecine extra-hospitalière

Looze, Vincent

Award date:
1991

Awarding institution:
Université de Namur

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Facultés
Universitaires
N.D. de la Paix
Namur

Institut d'Informatique

La transmission des résultats d'analyses médicales en médecine extra-hospitalière

par Vincent Looze

Promoteurs

Professeur J. Ramaekers
Docteur M. Beauloye

Mémoire présenté en vue de
l'obtention du grade de Licencié
et Maître en Informatique

Année académique 1990 - 1991

Résumé

Le médecin généraliste peut lorsqu'il en éprouve le besoin faire appel à un laboratoire d'analyses médicales. La transmission des demandes et des résultats se fait grâce à des formulaires spécifiques mais l'emploi de ceux-ci n'écarte pas totalement le risque d'erreurs dont les conséquences peuvent être très dommageables.

Les médecins s'informatisant, certains laboratoires envisagent de formaliser le texte des demandes et des résultats et d'automatiser et d'accélérer les transmissions en utilisant des systèmes informatiques de traitement et de transmission. Il est grand temps de se préoccuper des exigences à poser pour l'acceptation de tels systèmes garantissant ainsi le respect de règles juridiques, déontologiques et de sécurité tout en employant les meilleures techniques disponibles.

L'application des critères (correspondants aux exigences) à des systèmes existants ou en projet permet de les évaluer et d'en cerner et corriger les points faibles.

Abstract

Whenever the general doctor thinks it is necessary, he can call on a laboratory specialized in medical analysis. The transmission of these demands and the results is done by the means of specific formularies but the use of these do not exclude the risk of having errors with possible consequences that could be harmful.

Because of the wider use of computers in the world of medicine, some laboratories are thinking about installing a computer program that enables a quicker and more reliable use and transmission of the demands and results sheets. It is time to be preoccupied by the requirements that are necessary for the acceptance of these programs by ensuring the respect for the juridical, deontological and security rules while using the best techniques available.

The application of specific rules (which match the requirements) to programs that exist or that are in project enables the evaluation of these and therefore find and correct the weak points.

Remerciements

Je tiens ici à remercier toutes les personnes qui m'ont apporté leur précieux concours et plus particulièrement le Dr Beauloye M. et le professeur Ramaekers J. qui ont largement contribué au bon aboutissement de ce mémoire en acceptant de relire le texte, en faisant des remarques judicieuses et des suggestions opportunes et en me communiquant certains documents.

Avant-propos

Après avoir situé l'objectif du mémoire (chap I) et décrit la situation actuelle des échanges de résultats d'analyses médicales en médecine extra-hospitalière (chap II), le cadre général du problème est développé (chap III). L'étude en est subdivisée en quatre domaines particuliers: juridique, déontologique, technologique et sécuritaire. Ce chapitre peut être sauté par ceux ne désirant pas connaître les nombreux détails de la théorie et que seule l'exploitation des critères intéresse. Les deux parties les plus intéressantes de cette longue étude sont certainement celles concernant la cryptographie et la carte à microprocesseur.

Le chapitre IV reprend chaque critère tel qu'ils ont pu être dégagés de l'étude théorique. Une pondération leur est associée dans les tableaux récapitulatifs. Le cas échéant, ces pondérations sont commentées.

Enfin, trois systèmes existants sont décrits et confrontés aux listes de critères (chap V). Une tentative d'évaluation globale des trois systèmes et une explicitation de la démarche suivie constituent la conclusion.

I. Objectif	7
II. Collaboration médecin - laboratoire	8
A. Procédure actuelle	8
B. Améliorations possibles	8
C. Modes de transmission	8
1. L'utilisation du support papier	9
2. La conversation téléphonique	9
3. La transmission sur support magnétique	9
III. Cadre général	12
A. Aspects juridiques et déontologiques	12
1. La pratique médicale et la loi	12
2. La pratique médicale et l'informatisation	13
3. La sécurité et la loi	14
4. La déontologie médicale et son respect lors de l'introduction d'un système de transmission	15
5. Secret médical et secret informatique	16
B. Aspects technologiques	16
1. Transmission de la voix - Le réseau téléphonique	17
2. Réseaux informatiques	17
a. Réseaux privés	17
b. Réseaux publics	17
c. Architecture des réseaux d'ordinateurs	18
3. Transmission de textes	19
a. Télex	19
b. Télétex	19
c. Messagerie électronique	20
d. Télécopie	20
4. Transmission de données digitales	20
a. Réseau téléphonique commuté (RTC)	20
b. Liaisons analogiques spécialisées	20
c. Réseau DCS	21
d. Videotex	22
C. Aspects sécuritaires	22
1. Introduction	22
2. Les cibles d'attaques	24
3. Les motivations des agresseurs	25
4. Les risques dans le cadre de réseaux téléinformatiques	26
5. Les mesures de sécurité	27
a. Les mesures destinées à sauvegarder la confidentialité	27
b. Les mesures destinées à sauvegarder l'intégrité	28
c. Le chiffrement	29
6. La cryptographie	30
a. Généralités	30
b. Les chiffrements symétriques	31
c. Le Data Encryption Standard	42
d. Utilisation du chiffrement par blocs en pratique	45
e. Distribution des clés	49
f. Les chiffrements asymétriques (à clé publique)	50
g. La cryptographie et les réseaux	57
7. La carte à mémoire	58
a. Le concept de carte à microprocesseur	59

b. Les avantages de la carte à microprocesseur	63
c. Le cycle de vie d'une carte	65
d. Fonctionnement de la carte BULL CP8	66
e. La sécurité logique	73
f. Les applications des cartes à mémoire	76
g. Problèmes liés à la carte à puce	78
h. Evolutions	78
8. Les autres cartes	78
a. La carte à piste magnétique	78
b. La carte d'identification	79
c. Le bouchon	79
IV. Critères d'évaluation	81
A. Relevé des critères	81
1. Critères juridiques	81
2. Critères déontologiques	82
3. Critères technologiques	83
4. Critères sécuritaires	85
B. Règlement de la banque de données	87
C. Tableaux récapitulatifs et pondérations	89
1. Critères juridiques	89
2. Critères déontologiques	90
3. Critères technologiques	91
4. Critères sécuritaires	92
D. Commentaires	93
V. Réalisations	96
A. Le système du Dr Beauloye	96
1. Description du système	96
2. Système de boîtes aux lettres informatisées	97
3. Réglementation	99
a. La préservation du secret médical	99
b. Le libre choix du patient	99
c. La liberté et l'indépendance du médecin	99
B. Le système COBRA PC FAX	100
1. Description générale	100
2. Comparaisons avec le telefax	101
3. Fonctionnalités	102
a. du point de vue des facilités	102
b. du point de vue de la sécurité	103
c. du point de vue opérationnel	104
C. Le système TRASEC	105
1. Description générale	106
a. Modularisation	107
b. Le module d'authentification	107
c. La carte à microprocesseur	109
d. La gestion des mots de passe	109
e. Le terminal TRASEC	109
f. La validation et la génération de cartes	109
D. Evaluation de la solution du Dr Beauloye	111
1. Critères juridiques	111
2. Critères déontologiques	112
3. Critères technologiques	113
4. Critères sécuritaires	114

E. Evaluation de la solution MBLE	116
1. Critères juridiques	116
2. Critères déontologiques	117
3. Critères technologiques	118
4. Critères sécuritaires	119
F. Evaluation de la solution TRASEC	121
1. Critères juridiques	121
2. Critères déontologiques	122
3. Critères technologiques	123
4. Critères sécuritaires	124
VI. Conclusions	126

I. Objectif

Le médecin généraliste peut lorsqu'il en éprouve le besoin faire appel à un laboratoire d'analyses médicales. La transmission des demandes et des résultats se fait grâce à des formulaires spécifiques mais l'emploi de ceux-ci n'écarte pas totalement le risque d'erreurs dont les conséquences peuvent être très dommageables.

Les médecins s'informatisant, certains laboratoires envisagent de formaliser ⁽¹⁾ le texte des demandes et des résultats et d'automatiser et d'accélérer les transmissions. Cette formalisation ne peut réussir que si les médecins s'astreignent à un réel effort méthodologique et intellectuel pour se souvenir des règles scientifiques et déontologiques et pour les rendre conformes avec les exigences de rigueur de l'informatique [BEA]. La formalisation des informations échangées peut constituer une première étape à la constitution d'un Dossier Médical informatisé et plus tard à l'utilisation d'une carte santé individuelle. Ce problème ne sera pas abordé ici.

L'automatisation et l'accélération des transmissions est rendue possible par l'emploi de moyens informatiques et téléinformatiques: ordinateurs, réseaux de transmission,...

L'introduction de la téléinformatique et l'emploi de nouvelles techniques (réseaux, carte à mémoire, ...) entraînent un accroissement considérable des possibilités des systèmes de traitement de l'information mais aussi un risque d'insécurité par accès à distance aux données et aux programmes et un risque d'insécurité par accès aux données au cours de la transmission. Il est urgent de s'en préoccuper et d'étudier les exigences à poser pour l'acceptation de systèmes de traitement et de transmission.

Les praticiens et les biologistes désirant l'introduction de systèmes informatisés doivent obtenir l'accord de l'Ordre des Médecins. Celui-ci a adopté successivement plusieurs attitudes allant du refus catégorique à l'acceptation sous conditions, notamment le respect d'un règlement particulier [BE2].

Ce mémoire se propose d'étudier les critères à prendre en compte dans des systèmes informatisés d'échange de données entre laboratoires d'analyses biomédicales et cabinets médicaux.

⁽¹⁾ Par formaliser, on entend l'emploi de formulaires à rubriques bien définies et pour lesquels les mentions sont tirées d'une liste de réponses possibles.

II. Collaboration médecin - laboratoire

A. Procédure actuelle

Le médecin généraliste effectue un prélèvement (sachet de tubes) sur un de ses patients et l'envoie au laboratoire d'analyses bio-médicales, accompagné des renseignements relatifs au patient et relatifs au type d'analyses.

Le laboratoire effectue les analyses demandées, les résultats sont validés par un médecin biologiste et sont introduits dans un système informatique soit automatiquement (résultats de mesures automatisées) soit manuellement (intervention d'un opérateur). Ces mêmes résultats sont imprimés sur papier ou transférés sur disquette et transmis au médecin demandeur en respectant les précautions d'usage (respect du secret médical entre autres).

Ayant pris connaissance - éventuellement par ordinateur si la disquette est utilisée - et exploité les résultats, le médecin généraliste peut insérer les données dans le dossier du patient et poursuivre sa démarche.

B. Améliorations possibles

Trois points de cette procédure peuvent être améliorés:

- le formalisme des demandes et des résultats: le but recherché étant la correction des renseignements concernant le patient et le type d'analyses.
- la rapidité de transmission des résultats. Actuellement le réseau postal public ou privé étant utilisé, aussi bien pour le support papier que pour les disquettes, les délais sont de l'ordre de 1 à 2 jours.
- l'exploitation des résultats et leur report dans d'autres documents (Dossier Médical) qui se fait par réécriture manuelle (cas du support papier). L'emploi du support disquette permet lui une recopie informatique plus rapide et plus fidèle.

C. Modes de transmission

Trois modes de transmission sont actuellement utilisés:

- l'utilisation du support papier
- la conversation téléphonique
- la transmission sur support magnétique

1. L'utilisation du support papier

Il s'agit là du mode de transmission le plus courant et le plus simple: il ne demande en effet que peu d'investissements. Il est également le seul reconnu officiellement. De plus le compte-rendu signé par le biologiste a valeur légale et est le seul l'engageant.

Néanmoins, comme pour toutes les opérations requérant une intervention humaine, les erreurs sont toujours possibles: fautes de frappe lors de l'identification du patient ou même malentendus causés le plus souvent par un manque de formalisme.

Afin de sauvegarder le secret, le compte-rendu doit être transmis sous enveloppe scellée (conditionnement particulier) et à une adresse précise. L'utilisation du réseau postal entraîne des délais de l'ordre de 1 à 2 jours.

2. La conversation téléphonique

Un des avantages fréquemment évoqué de la transmission des résultats par téléphone est sa rapidité. Il faut néanmoins tenir compte du fait que le médecin généraliste doit être présent lors de l'appel ce qui n'est pas souvent le cas, le médecin généraliste effectuant souvent des visites à domicile.

D'autres inconvénients peuvent être mis en avant:

- l'identité des interlocuteurs n'est jamais certaine
- la transmission orale entraîne de nombreuses déformations de l'identité du patient ou des paramètres transmis

Ce mode de transmission a toutefois l'énorme avantage de permettre un dialogue direct entre le laboratoire et le médecin généraliste et ne peut pour cette raison être totalement rejeté mais dans tous les cas le choix de ce mode doit être réservé au médecin biologiste.

3. La transmission sur support magnétique

L'emploi de supports magnétiques (essentiellement des disquettes) permet une plus grande confidentialité grâce à l'utilisation de fichiers compactés et chiffrés.

Il permet également l'intégration, la mise à jour constante du Dossier biologique par simple échange de supports et la mise à jour rapide par report dans le Dossier Médical si celui-ci est informatique.

La conservation des données biologiques au laboratoire est plus facile (encombrement moindre, accès plus aisé). La durée de conservation des données sur support magnétique n'est cependant pas infinie: il faut veiller à en faire au minimum deux copies et

à les vérifier périodiquement (une fois par an par exemple).

La documentation des résultats est au moins de qualité égale à celle du support papier.

Ce mode de transmission a toutefois quelques défauts déjà évoqués pour le premier mode:

- si le réseau postal public est utilisé, les délais sont de l'ordre de 1 à 2 jours
- si le laboratoire se charge lui-même de la distribution, la charge de travail de son personnel s'en trouve augmentée
- les transports postaux public ou privé peuvent endommager physiquement (chocs, influences électromagnétiques, variation de température, pliage des disquettes) les supports les rendant alors illisibles (fragilité du support).

Les erreurs d'identification du patient ou les malentendus sont toujours possibles, le même fichier servant à la copie sur disquettes et à l'impression sur papier. Cependant, l'emploi de supports magnétiques couplé à une gestion informatisée du dossier médical permet un contrôle automatique de l'identité (refus d'insertion si les nom, prénom et date de naissance ne correspondent pas) ce qui diminue déjà fortement le nombre d'erreurs.

<u>Support papier</u>	
Avantages	Inconvénients
peu d'investissements valeur officielle	erreurs possibles conditionnement particulier délais
<u>Transmission téléphonique</u>	
Avantages	Inconvénients
rapidité dialogue direct	disponibilité du médecin généraliste exigée identité incertaine déformations
<u>Support magnétique</u>	
Avantages	Inconvénients
confidentialité intégration facilité de stockage documentation	erreurs possibles (réduites si le dossier médical est informatisé) délais ou charge de travail accrue fragilité altération possible au cours du temps

tableau 1: Comparaison des modes de transmission

III. Cadre général

L'objectif des critères d'évaluation à prendre en compte pour les systèmes informatisés (I) est double:

- garantir le respect des principes d'éthique médicale (aspects juridiques et déontologiques)
- assurer la sécurité et la fiabilité globale du système (aspects technologiques et sécuritaires).

A. Aspects juridiques et déontologiques

Les textes qui régissent le secret de données médicales sont de deux types: certains expriment une déontologie, c'est-à-dire des règles à observer, des devoirs à accomplir, d'autres sanctionnent les infractions, ce sont des textes à caractère pénal. Ils relèvent également d'une double tradition: l'une qui remonte aux origines de la médecine, celle du secret professionnel qui oblige médecins et professions associées, l'autre beaucoup plus récente qui concerne le respect de la vie privée sous toutes ses formes et donc à titre de cas particulier la santé des personnes. La forme la plus élaborée de cette seconde tradition est en France la loi du 6 janvier 1978 sur "l'Informatique, les fichiers et les libertés". Cette loi crée le secret informatique.

1. La pratique médicale et la loi

Le secret médical est un des principes fondamentaux de la pratique médicale. Il suscite un climat de confiance entre le patient et son médecin. Le médecin n'est pas chargé par la société de prêter des soins, il est l'objet de la confiance d'un individu et ses premiers devoirs visent à la protection de son intégrité individuelle. Le respect du secret a comme raison d'être de garantir le respect de la personne humaine, de son intimité et de son droit à une vie privée. Ses violations toucheraient donc aux bases de la société démocratique actuelle. En Belgique, le secret médical est garanti par l'article 458 du Code Pénal.

Le secret a un caractère absolu. Les médecins, paramédicaux et toutes autres personnes qui de par leur profession ou leur état reçoivent des informations médicales sont tenues au respect du secret. En cas de violation, les personnes dépositaires du secret seront condamnées à une peine d'emprisonnement de 6 mois maximum et d'une amende de 500 F au plus.

Le secret couvre toutes les informations confiées par le patient et celles que le médecin a surpris à l'occasion de ses visites, même celles qui seraient sans rapport avec sa profession. Le délit doit être volontaire, tout oubli ou négligence ne serait passible que de sanctions disciplinaires mais il

existe en dehors de tout préjudice causé au patient. Dans l'intérêt du patient, il est prévu un partage indispensable du secret au sein de l'équipe médicale. Ces collaborateurs sont naturellement soumis au respect du secret. Le médecin doit avoir le consentement du patient pour transmettre son fichier à un autre médecin (médecin reprenant son cabinet, par exemple).

Il existe certaines dérogations au principe du secret médical si elles sont justifiées par un intérêt d'ordre supérieur, si elles sont nécessaires à la sécurité, à la protection de la santé ou à la morale et à la protection des droits d'autrui (déclarations de maladies vénériennes, de maladies contagieuses, déclarations de naissance, témoignages en justice,...). Mais comment arriver à satisfaire une mesure d'intérêt collectif sans préjudicier l'individu, étant donné que la limite de cet intérêt collectif n'est pas facile à définir ? L'intérêt du patient demande à la fois le respect de sa vie privée et une intervention médicale la plus rapide possible en cas d'accident, ce qui signifie l'accès instantané à certaines données nécessaires, notamment le groupe sanguin ou concernant les personnes diabétiques, le type de diabète présenté, pour faciliter une intervention d'urgence. Mais face à cet objectif justifié, on comprend l'effet discriminatoire que peut avoir la connaissance d'un état pathologique pour un employeur et l'énorme difficulté de départ à définir cet intérêt collectif et ses effets pervers non escomptés.

2. La pratique médicale et l'informatisation

Dans la pratique médicale actuelle, le secret médical s'est conceptuellement transformé. Si, au départ, il est la base du climat de confiance qui unit le médecin à son patient, par l'informatisation du dossier médical les données contenues ne sont plus seulement manipulées par le médecin traitant, sa secrétaire ou par une équipe médicale, mais par de nouveaux auxiliaires qui encodent les données et programment le traitement de ces informations: l'informatique médicale implique la collaboration de nombreuses personnes appartenant à d'autres professions non médicales qui ne sont pas toutes tenues au secret professionnel. Il y a donc transfert de responsabilités entre la profession médicale et d'autres professions, de sorte que les risques d'indiscrétions constituent un danger réel. Le problème pourrait être résolu si le médecin était obligé de connaître un minimum d'informatique, minimum nécessaire et suffisant à la "neutralisation" des données lors des interventions techniques.

Le caractère absolu du secret médical ne peut plus être garanti dans l'exercice de la médecine moderne. Il faut le partager pour des motifs médicaux ou sociaux. L'introduction de l'informatique qui facilite l'accès aux informations et la rapidité des transmissions, qui multiplie les points d'accès et per-

met le stockage, la centralisation et le collationnement des données dans de larges proportions, doit être assortie de garanties spécifiques qui permettront de sauvegarder, dans le partage du secret, sa confidentialité.

3. La sécurité et la loi

La loi est un domaine ancien puisqu'elle existe depuis toujours. L'informatique quant à elle est toute récente. Elle n'a que peu de relations avec la loi. Mieux encore, les spécificités de l'informatique font que la loi est une matière qui s'adapte difficilement à l'informatique. Le législateur doit assurer sa mission, en l'espèce faire respecter l'ordre en prenant des mesures de nature à résoudre les problèmes qui pourraient découler de l'atteinte à la sécurité des systèmes informatiques. Même si le législateur a cherché à offrir à l'informatique un ensemble de lois permettant aux utilisateurs de cette nouvelle technique de disposer de moyens de sanctions, force est de constater que l'objectif n'est que partiellement atteint. En effet, il est difficile d'associer la loi à ce domaine particulier qu'est la sécurité informatique. Cela tient plus à l'inadéquation des moyens de preuves traditionnellement reconnus par la loi qu'à la reconnaissance par le juge de l'existence de délits informatiques.

La Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement des données à caractère personnel décrit les principes généraux à respecter:

- la confidentialité des données est nécessaire au respect de la vie privée
- les données doivent être obtenues et traitées loyalement et licitement
- chacun doit pouvoir consulter et faire corriger les données le concernant (cette correction doit évidemment être justifiée)
- la finalité de la collecte de données doit être connue et vérifiée. Les données doivent être adaptées à cette finalité
- les données doivent être exactes et mises à jour
- la durée de conservation des données ne doit pas être excessive

La Convention du Conseil de l'Europe exige la tenue d'un registre centralisé de toutes les banques de données contenant des informations personnelles.

4. La déontologie médicale et son respect lors de l'introduction d'un système de transmission

Une déontologie, c'est l'ensemble des règles qui doivent régir la conduite d'une profession. L'esprit de la déontologie médicale retient le respect de la liberté, le respect de la vie, le respect de la personne. Pour ce qui concerne le secret, la déontologie de la profession remonte au moins à Hippocrate: "Les choses que, dans l'exercice ou même hors de l'exercice de mon art, je pourrai voir et entendre sur l'existence des hommes, et qui ne doivent pas être divulguées au dehors, je les tairai, estimant que ces choses-là ont droit au secret des mystères". Cette loi morale est codifiée par des textes législatifs.

Le Conseil National de l'Ordre des Médecins formule une éthique et promulgue les règles à respecter en matière d'échanges d'informations informatisées entre les laboratoires de biologie médicales, les médecins praticiens et les patients. Cet Ordre est donc un point de passage obligé pour la mise en place d'un système de transmission.

Outre le respect du secret médical, il faut aussi garantir la liberté de choix du patient: choix du laboratoire et choix du mode de transmission des résultats.

De plus, le laboratoire ne peut avoir accès aux Dossiers médicaux du médecin prescripteur et le médecin ne peut avoir accès aux résultats qui ne concernent pas ses patients (cloisonnement des Dossiers médicaux).

Le malade devra être informé que le laboratoire et le médecin généraliste sont équipés d'un ordinateur et que, sauf avis contraire de sa part, le médecin demandeur de ces examens aura accès à ses résultats. Le malade aura aussi la possibilité de donner le nom d'autres médecins qu'il désigne à cet effet. Le Dossier malade devra donc permettre la saisie de plusieurs médecins traitants.

Pour être accessible, le dossier d'un malade devra obligatoirement avoir été validé par le médecin biologiste du laboratoire et cela de façon apparente dans le dossier du malade. Des textes libres doivent pouvoir être introduits et certains résultats doivent pouvoir être mis en évidence.

Une des particularités de la profession médicale est qu'un meilleur traitement de l'information (tenue à jour informatisée de dossiers médicaux, transmission de résultats par réseaux,...) ne peut constituer un argument de choix par le patient d'un médecin préférentiellement à un autre. Autrement dit, on ne peut considérer l'informatisation comme un critère de qualité. Le service ainsi rendu ne peut non plus être payant. On ne peut toutefois nier que l'informatisation favorise une meilleure

gestion des données, le médecin attachant alors plus d'importance à ces données objectives et ne se basant pas uniquement sur son jugement.

5. Secret médical et secret informatique

De par la loi le secret informatique s'ajoute aux exigences du secret médical. Il importe donc de bien saisir la différence entre les deux. Le secret professionnel vise des personnes appartenant à des professions bien définies: les confidents nécessaires de l'acte médical et il ne concerne pas les informaticiens qui ne font pas partie prenante de cet acte. Le secret informatique concerne des objets, à savoir les données concernant les personnes fichées et il s'impose à tous ceux qui peuvent avoir accès aux fichiers donc au premier chef aux informaticiens. Le secret professionnel est absolu et le malade ne peut en délier le médecin. Celui-ci peut être poursuivi et condamné même sans préjudice, même sans plainte. Le Code pénal exige un acte volontaire et il écarte imprudence et négligence, par exemple celle de laisser traîner des papiers confidentiels. La loi relative à l'informatique, aux fichiers et aux libertés (France) est beaucoup plus sévère. Elle prévoit des sanctions en cas de divulgation même par imprudence ou par négligence.

B. Aspects technologiques

De la rencontre entre l'informatique et les télécommunications est née la téléinformatique. On considère généralement que le terme service téléinformatique englobe tous les services hormis la téléphonie. Le facsimile, le télex, le télétexte et le vidéotexte en sont quelques exemples.

La téléinformatique, pour transmettre des informations, fait le plus souvent appel à une architecture particulière: celle des réseaux.

Un réseau apparaît sitôt que plusieurs sources et/ou plusieurs destinataires (permanents ou potentiels) se partagent le même service. Le réseau est constitué d'un ensemble de voies de transmission similaires, ainsi que des moyens nécessaires pour les relier entre elles et les attribuer aux usagers. L'attribution de voies de transmission aux usagers est appelée assignation. L'assignation est fixe (statique) ou variable (dynamique). Dans ce dernier cas, une opération de commutation est nécessaire.

Pour des raisons économiques, le réseau commuté est le plus souvent réalisé sous forme banalisée, c'est-à-dire sous forme communautaire. Dans un tel réseau, seule la voie qui relie l'utilisateur au réseau est individuelle.

1. Transmission de la voix - Le réseau téléphonique

Le réseau à commutation de circuits de loin le plus répandu est le réseau public de télécommunications - le réseau téléphonique. Il est actuellement constitué d'une série de réseaux nationaux interconnectés entre eux pour former un réseau international. Même s'il a été à l'origine conçu pour opérer avec des appareils téléphoniques analogiques, il traite aussi un important trafic de données digitales via des modems. Sa conversion en un réseau digital est en cours. En Belgique, l'infrastructure du réseau est sous monopole de la RTT.

La plupart des abonnés du réseau sont des appareils téléphoniques. Ces appareils sont constitués d'un émetteur convertissant la voix (analogique, ondes sonores) en signaux électriques (analogiques, fréquences de 300 à 3400 Hz) et d'un récepteur effectuant l'opération inverse.

2. Réseaux informatiques

a. Réseaux privés

Mis à part les cas particuliers où l'utilisateur privé dispose de ses propres lignes (réseaux informatiques domestiques ou locaux), les réseaux informatiques privés sont constitués

- de moyens de transmission empruntés au réseau de télécommunication public (circuits loués,...)

- de centres de commutation (de circuits, de messages ou de paquets) qui leur sont propres et sont adaptés aux besoins particuliers de la commutation de données.

Ils représentent donc une alternative à l'utilisation de circuits commutés à travers le réseau (téléphonique ou télex) public. Les frais de location des circuits ne se justifient qu'en cas de trafic important. Le taux d'occupation des circuits loués peut être avantageusement amélioré par un multiplexage fixe ou, mieux encore, dynamique (concentration de trafic).

b. Réseaux publics

Par leur nature même, les réseaux privés sont restreints à un cercle fermé d'utilisateurs. De plus, ils sont généralement incompatibles entre eux, pour des raisons de protocoles et de logiciel.

Un réseau informatique public, analogue au réseau téléphonique existant, se propose de

- couvrir sur une base nationale et internationale les be-

soins en téléinformatique d'utilisateurs de différentes catégories (privés, professionnels, grand public)

- offrir des services banalisés de transmission, de commutation et de stockage d'information efficaces, souples et économiques

- garantir une certaine universalité dans les débits, les formats et les modes d'exploitation des terminaux raccordés au réseau

- permettre une évolution qualitative et quantitative des besoins.

Un gros effort de normalisation a été fait par l'ISO (International Standard Organization) et par le CCITT (Avis de la série X) dans le but de prévenir les incompatibilités et les options funestes.

c. Architecture des réseaux d'ordinateurs

Tant que seule la transmission de la voix est exigée, la liaison physique ou la mise à disposition par un réseau de communication de capacités de transmission partagées par de multiples stations était suffisante. Mais dès que l'on désire transmettre des données, il faut implémenter une série de fonctions permettant de remplir cette tâche efficacement. Ces diverses fonctions sont classées suivant une certaine architecture. Une des plus célèbres de ces architectures est le modèle OSI (Open System Interconnection) de l'ISO.

Pour que deux entités puissent communiquer, elles doivent parler le même langage, c'est-à-dire que l'échange doit être conforme à un certain nombre de conventions acceptées par toutes les parties. L'ensemble de ces conventions est appelé un protocole. Les éléments principaux d'un protocole sont:

- la syntaxe: le format des données, le codage, le niveau des signaux,...

- la sémantique: les informations de contrôle pour la coordination et le contrôle d'erreurs,...

- la synchronisation: adaptation des vitesses et séquençement

La prise en charge de tous les problèmes de communication pour toutes les configurations possibles est un problème beaucoup trop vaste que pour être résolu en une seule fois. C'est pour cette raison qu'un modèle en couches ou hiérarchisé a été introduit. Des fonctions primitives, de bas niveau sont implémentées sur des entités de bas niveau, four-

nissant des services aux entités de plus haut niveau.

Le modèle OSI est constitué de sept couches distinctes: physique, liaison de données, réseau, transport, session, présentation et application. La communication est assurée par deux entités de la même couche, situées chacune dans un des systèmes reliés. Il faut noter qu'il n'y a communication directe que via la couche physique.

Outre cette découpe en couches, l'emploi de standards est nécessaire. Ces standards définissent les protocoles utilisés entre les entités de même niveau.

Quelques exemples de standards:

Couche physique: RS-232, RS449/422/423, X.21 (partiel)
Couche liaison de données: HDLC, BSC
Couche réseau: X.25, X.21 (partiel)

3. Transmission de textes

a. Téléx

Le service Téléx est destiné à la transmission pure et simple de textes. Son utilisation connaît actuellement une certaine régression vu la croissance d'outils plus modernes. Le réseau Téléx est étendu au monde entier. La transmission se fait à la vitesse faible de 50 bps (7 caractères par seconde). Un ordinateur peut être connecté au réseau.

b. Télétex

Le service Télétex regroupe le traitement de textes et leur transmission. Il assure le transfert entre mémoires de systèmes informatiques à la vitesse de 2400 bps. L'interface de communication est intégré dans le poste de travail. Celui-ci est fourni en concurrence par la RTT et des constructeurs privés.

Le réseau de transport utilisé est le réseau DCS (voir III.B.4.c). L'interfonctionnement avec le réseau Téléx est possible. De plus, le poste peut accéder à d'autres services offerts par DCS tel l'interrogation de bases de données.

Ce service pourrait devenir, avec la télécopie, un outil essentiel de transmission du courrier d'affaires. Une extension intéressante, dite "mode mixte" permettra d'assurer la transmission de documents contenant des textes et des images.

c. Messagerie électronique

Accessible depuis fin 1984, le service de messagerie DCSMail permet à tout utilisateur du réseau DCS l'accès à un système informatique de "boîte aux lettres" dans lequel il peut stocker des messages pour certains autres abonnés, consulter la liste des messages qui lui sont destinés et prendre connaissance de leur contenu. Ce service assure la multidiffusion, l'archivage et la destruction des messages. A court terme, il sera intégré dans un réseau public international de messagerie électronique répondant à la norme X.400.

d. Télécopie

Les appareils de télécopie (ou Telefax) permettent d'émettre et de recevoir via le réseau téléphonique commuté des copies de documents quelconques selon un procédé de photocopie à distance. Ces équipements peuvent fonctionner de façon plus ou moins autonome. Ils répondent à des normes et permettent des transmissions internationales. Le temps nécessaire à la transmission d'un document A4 est de l'ordre de la dizaine de secondes.

4. Transmission de données digitales

Les données binaires peuvent être transmises telles quelles sur des liaisons numériques spécialisées ou être véhiculées sur des liaisons analogiques au prix du passage par un modulateur-démodulateur (modem).

a. Réseau téléphonique commuté (RTC)

La RTT assure via le RTC un service de transmission de données de qualité et de vitesse moyennes. D'après le choix des modems, les vitesses s'échelonnent entre 300 et 4800 voire 9600 bps. La qualité de la transmission n'est pas garantie par la RTT qui laisse à l'utilisateur le soin de prendre les mesures de protection nécessaires contre les erreurs de transmission. Les modems sont fournis ou agréés par la RTT.

Typiquement, on utilise le RTC pour des liaisons essentiellement temporaires portant sur des messages de courte taille et peu sensibles aux erreurs éventuelles.

b. Liaisons analogiques spécialisées

Dans la mesure des possibilités de la Régie et dans les limites de la réglementation, d'ailleurs en évolution, un utilisateur peut louer à la RTT des liaisons reliant en permanence un site quelconque du territoire national avec un autre site belge ou étranger.

Ces liaisons permanentes et point-à-point peuvent être de qualité standard (norme 1040) ou de qualité supérieure (normes 1020 et 1025). Equipées des modems adéquats, ces liaisons peuvent permettre des vitesses plus élevées que le RTC (jusqu'à 19200 bps) avec un meilleur taux d'erreurs.

Ce type de liaison répond bien aux besoins lorsque les correspondants sont fixes et, surtout, s'ils doivent être accessibles de façon permanente.

c. Réseau DCS

Le réseau DCS (Data Communication Service) est un réseau public commuté exclusivement destiné aux transmissions de données digitales. Il est constitué d'un certain nombre de liaisons numériques à grande vitesse reliant des noeuds de commutation. Il est accessible par des lignes analogiques équipées de modems exclusivement fournis par la RTT. Le principe utilisé est la commutation de paquets.

Les abonnés peuvent accéder au réseau de quatre manières:

- soit par une liaison permanente respectant le protocole synchrone X.25 et permettant des vitesses de 2400, 4800, 9600 et 48000 bps
- soit par une liaison permanente vers un équipement public d'assemblage et de désassemblage de paquets (PAD), selon le protocole asynchrone X.28 et pour des vitesses de 300 et 1200 bps
- soit par le RTC vers le PAD
- soit par le réseau Téléex vers le PAD

Les principaux avantages du DCS sont:

- l'interconnectabilité d'appareils différents avec adaptation des vitesses
- la bonne protection contre les erreurs
- la possibilité de créer plusieurs connexions simultanées sur une liaison d'accès
- la possibilité de créer des circuits permanents
- la grande disponibilité
- la tarification indépendante de la distance
- la connexion à de nombreux réseaux étrangers

Typiquement, l'utilisation du DCS s'impose si l'on désire transmettre des messages de manière rapide et fiable sur une base non permanente et à des interlocuteurs variables.

d. Videotex

Le videotex est un service télématique permettant la consultation de banques de données et l'accès à différents services interactifs à partir d'équipements terminaux de coût faible et au moyen du RTC. Les terminaux sont principalement de trois types: récepteur de télévision adapté et équipé d'un modem, terminal Videotex spécifique (type Minitel) ou ordinateur PC avec carte spéciale.

C. Aspects sécuritaires

1. Introduction

Notre société devenant de plus en plus dépendante des réseaux informatiques et les données transmises étant de plus en plus nombreuses, la menace d'interférences délibérées avec ces systèmes grandit.

L'emploi de moyens informatiques pour la transmission de résultats rend nécessaire la prise de mesures de sécurité. Ces mesures visent à la limitation des risques et sont le fruit d'un compromis entre objectif réaliste et coût des moyens. Un des objectifs réalistes les plus communément retenus est d'atteindre un degré de sécurité au moins aussi bon que celui atteint avant l'introduction des systèmes informatiques. Il est à noter que le degré de sécurité informatique est déterminé par le degré de sécurité de son élément le plus faiblement protégé.

L'introduction du télétraitement dans tous les domaines des affaires, du commerce et de l'industrie engendre de nouveaux problèmes de sécurité. Les transactions bancaires électroniques ont été les premières applications attaquées (spectaculaires fraudes sous la forme de transferts de fonds falsifiés, par exemple). Les banques, de plus en plus suivies par les autres secteurs, ont alors appliqué les méthodes modernes de sécurisation.

La destruction des sécurités est pour certains un défi. Cette pratique, certes peu recommandable, a néanmoins eu le mérite de rendre les responsables de la sécurité conscients de la nécessité de mesures de protection. Une des caractéristiques principales des attaques illégales contre les ordinateurs est qu'elles n'engendrent pas de sentiment de culpabilité. La loi, dans la plupart des pays, ne traite pas ce genre de délit. En l'absence de sanctions, le test des défenses d'un système est considéré comme un jeu mais il peut aussi devenir l'instrument de crimes organisés.

Certains pays ont toutefois établi une législation assurant un degré raisonnable de protection de la vie privée, d'autres la prépare. Le texte de ces nouvelles lois peut être utilisé com-

me référence pour l'implémentation de techniques de protection.

La démarche est essentiellement pragmatique en ce sens que seule l'insécurité d'un système peut être démontrée, sa sécurité étant alors "démontrée" par l'absence de failles. Personne ne peut donner une garantie absolue. La possibilité d'apporter une preuve n'existe que dans de très rares cas.

Optimiser l'efficacité ou le coût d'un système est souvent facilement exprimable, il suffit de maximiser ou minimiser une certaine fonction, complexe sans doute, mais au moins la structure mathématique du problème est connue. Par contre la construction d'un système optimisant la sécurité fait appel à des notions de la théorie des jeux: il s'agit d'analyser un système où deux opposants pensent chacun indépendamment à leur stratégie. Le résultat de l'affrontement est une conséquence de leurs choix.

Il est très difficile d'énumérer toutes les sortes d'attaques. Premièrement, il faut estimer les motifs et intentions de l'ennemi: les informations volées peuvent être utilisées pour frauder, espionner, en tirer des avantages commerciaux, exercer un chantage,... Les parades à ces attaques ne sont pas toujours identiques: coder l'information d'une bande magnétique peut la rendre inutilisable à l'ennemi mais s'il n'en existe qu'un seul exemplaire, elle peut faire l'objet d'un chantage.

La diversité des attaques possibles rend la protection difficile. Il est peu probable qu'une méthode systématique d'analyse soit trouvée mais des listes de contrôle peuvent être utiles.

Il n'est pas habituel d'avoir une description d'un système d'information si précise qu'il est possible d'en identifier toutes les faiblesses potentielles. Dès lors, un bon investigateur travaille à partir d'entretiens avec ceux qui connaissent le mieux le système et non à partir de papiers et de spécifications.

Nous considérons qu'un système est sécurisé si nous avons été incapables de trouver une méthode donnant un certain avantage à l'attaquant. Mais nous pouvons avoir échoué dans l'identification de la nature de l'ennemi ou avoir oublié une certaine méthode d'attaque. Une évaluation de la qualité de la sécurité ne doit jamais se baser sur la démarche de conception du développeur. Il a certainement pensé à la sécurité et s'est convaincu lui-même que tous les aspects avaient été couverts. Il a probablement de bonnes raisons de le croire mais il faut aborder le système de manière différente, trouver d'autres approches: le développeur a pu concentrer son attention sur certaines parties du système et en avoir oublié d'autres. D'autre part les systèmes sont tellement complexes que seuls ceux qui les ont implémenté peuvent les connaître parfaitement en détail. Les

implémenteurs doivent être intégrés dans l'étude de sécurité. Ils doivent être convaincu qu'il existe des failles et être persuadés de les rechercher.

2. Les cibles d'attaques

Deux parties sont particulièrement sujettes aux attaques: le logiciel et les personnes opérant sur le système. Le logiciel d'un système d'information conditionne souvent sa complexité, le matériel étant lui simple et composé principalement d'unités standards telles les microprocesseurs et les mémoires. Une des qualités du logiciel est qu'il peut être modifié durant le développement ou par après afin de donner au système de nouvelles propriétés. Cette flexibilité est aussi une menace sérieuse pour la sécurité du système.

Des outils spéciaux ont été conçus pour aider les programmeurs à modifier leurs programmes à différents niveaux. Ces outils sont très dangereux particulièrement si le programmeur travaille pour un ennemi. Garder ces outils quand le logiciel est en opération constitue une faiblesse majeure du système parce qu'ils permettent des modifications ultérieures qui peuvent introduire des trappes délibérées dans les parties s'occupant de la sécurité du système. La meilleure solution est de garder une ou deux versions avec ces outils de programmation pour le test logiciel et la mise à jour mais les versions tournant réellement et allant en dehors d'un milieu sécurisé doivent être aussi hermétiques que possible.

Les systèmes basés sur les microprocesseurs sont sujets à une menace particulière car ils utilisent des mémoires mortes qu'un agresseur peut changer, la nouvelle mémoire morte simulant le fonctionnement normal et en même temps remplissant une fonction d'écoute particulière. Cette attaque peut être rendue plus difficile en s'assurant que le programme remplisse tout l'espace disponible en mémoire morte et en fixant la mémoire morte au lieu de la poser sur les supports.

Des trois opérations principales effectuées par un système d'information (stockage, traitement et transmission), c'est indubitablement la transmission qui est la plus vulnérable. Un réseau de communication est constitué de nombreux câbles, liaisons radio, interrupteurs, multiplexeurs répartis dans de nombreux lieux, toutes ces parties de systèmes étant des cibles potentielles. Il est impossible de sécuriser un réseau étendu, les mesures de sécurité dépendent de techniques de traitement de l'information dont la cryptographie.

Les données stockées sont aussi l'objet d'attaques parce que le temps de stockage est nettement supérieur au temps de traitement. La protection des données stockées peut utiliser des techniques de cryptographie.

Aucun système ne peut être sécurisé sans protection physique d'une partie de ses équipements. Le tout est de concentrer le besoin de sécurité physique, pas de l'éliminer complètement. De plus, le traitement des données requiert qu'elles soient reçues en clair, ce qui exige une protection des organes de traitement contre les intrusions.

Dans de nombreux systèmes, les données et les opérations demandant le plus haut degré de sécurité peuvent être contenues dans un boîtier de dimensions réduites, physiquement résistant et conçu de façon à détruire les secrets y stockés quand on l'ouvre. C'est l'élément central des systèmes sécurisés.

Une des démarches à suivre pour assurer une bonne protection logique est la suivante:

- procéder à une identification des risques et à leur évaluation
- choisir les mesures préventives de protection qui correspondent aux risques auxquels on veut, on peut, on doit faire face.
- reconnaître les risques auxquels on ne peut faire face
- mettre en place les mesures de rattrapage et de correction
- souscrire les assurances nécessaires.

3. Les motivations des agresseurs

Un agresseur en informatique peut être un fraudeur au sens habituel du terme. Cela signifie qu'il agit avec l'intention de tromper en commettant un acte de mauvaise foi. Cependant, la criminalité qui le caractérise présente une certaine spécificité dans la mesure où elle s'exerce dans un domaine particulier.

Un certain nombre de motivations peuvent être évoquées, permettant de mieux cerner les raisons qui expliquent qu'un individu puisse devenir un fraudeur potentiel.

- le défi: au même titre qu'une ascension au cours de laquelle le grimpeur se lance un défi à lui-même en même temps qu'il attaque les premiers versants de la montagne. Le défi lancé alors à la montagne ressemble, à bien des égards, à celui lancé au système informatique.

- le désir de jouer: que ce soit un match de tennis ou le jeu au casino, la participation du joueur peut être très forte tant la passion est grande et l'appât de la victoire et de la gloire irrésistible.

- la folie: disposer de l'ordinateur, c'est être en mesure de provoquer des actes insensés, irréfléchis, susceptibles de mettre en péril la survie du système.

- l'argent: l'aspect financier ne peut être écarté: l'escroquerie, le détournement de fonds, voire la vente de fichiers de données secrètes peuvent tenter de nombreux malfaiteurs.

- les sentiments personnels: l'agresseur en informatique peut, à un instant déterminé, avoir des pensées plus ou moins nuisibles. Animé soit d'un sentiment de frustration, de laissé-pour-compte, d'injustice, soit d'un esprit de vengeance, voire, dans certains cas, de vandalisme, soit pis encore, de pensées plus perverses ressemblant fort à celles d'idéologues ou de terroristes, le fraudeur peut se livrer à des malversations endommageant l'intégrité et la confidentialité des données du système.

Toutefois la probabilité de réalisation d'une attaque de nature informatique dépend de plusieurs conditions essentielles:

- du gain escompté de la fraude dans le cas de succès de l'attaque
- du niveau de connaissances techniques requis pour mener à bien la tentative
- du coût de réalisation de la dite tentative comparé au gain attendu et éventuellement produit
- des sanctions encourues par le fraudeur en cas d'identification
- du délai maximum imparti pour exécuter la fraude
- de l'image de marque procurée par un succès potentiel
- du niveau de complexité de l'attaque, cette complexité augmentant en fonction du nombre de programmes à modifier, du nombre d'individus impliqués, du mode de répartition des données confidentielles, des niveaux de protection.

Il faut enfin savoir que s'agissant du domaine informatique, pour être fraudeur, il faut pratiquement toujours être soi-même informaticien ou au moins être doté de compétences techniques reconnues.

4. Les risques dans le cadre de réseaux téléinformatiques

L'emploi de la téléinformatique pose des problèmes qui sont dus à la nature des informations transmises et aux caractéristiques du mode de transmission.

Les risques sont assez nombreux. Les menaces précitées sont toujours valables. Néanmoins, alors que dans une attaque locale par un tiers le fraudeur peut s'assimiler à un cambrioleur (il prend par conséquent autant de risques de se faire repérer visuellement que s'il volait un dossier), dans le cas d'une attaque à distance il préserve son anonymat et le flagrant délit est impossible. La difficulté pour le fraudeur est alors de pénétrer le système à distance mais il dispose de certaines méthodes dont la détection est très difficile.

Il peut opérer la recherche systématique du n° d'accès puisque certains appareils permettent de détecter l'existence d'une porteuse (c'est-à-dire l'existence d'un ordinateur). Un pirate équipé d'un système d'appel automatique peut composer les numéros de téléphone de façon systématique et accéder aux ordinateurs.

Une fois l'ordinateur repéré, le fraudeur va chercher des identifiants et les mots de passe associés afin d'entrer dans le système informatique. Un programme relativement simple permet une recherche systématique des identifiants et des mots de passe utilisés.

5. Les mesures de sécurité

Les techniques de protection de données tentent de prévenir le vol d'information. Elles ont connu un fort développement ces dernières années. Il n'existe cependant pas de solution miracle pour se prémunir contre les attaques exposées ci-dessus, mais on peut diminuer les risques en prenant un minimum de précautions. Celles-ci doivent être adaptées que ce soit sur le plan technique ou organisationnel et il n'est pas possible de dégager une méthode universelle puisque chaque système est un cas particulier.

La sécurité au niveau physique est assurée par le respect de précautions normalement prises contre les risques courants: vol, incendie, inondation, intrusion ainsi que de quelques autres: propreté des équipements, stabilité de l'installation électrique, sauvetage fréquent des fichiers.

La définition de mesures standards au niveau logique est malaisée. On peut toutefois en retenir quelques-unes:

a. Les mesures destinées à sauvegarder la confidentialité

La confidentialité d'un message est assurée si seules les personnes autorisées peuvent en prendre connaissance. Cela revient donc à un contrôle d'accès aux données, contrôle devenu particulièrement important depuis l'avènement des processus en temps partagé et l'utilisation de réseaux. Il faut pour cela:

- vérifier les identités
- l'autorisation d'accès ne peut être accordée qu'à un utilisateur identifié
- l'accès aux fichiers doit être contrôlé pour chaque utilisateur autorisé
- les partenaires d'un échange doivent se reconnaître mutuellement
- les intrusions dans les communications doivent être empêchées

Généralement l'accès est contrôlé par un ensemble de mesures, celles-ci ne donnant des droits (sur des matériels, des fonctions, des informations) qu'aux seules personnes ou matériels autorisés.

Le contrôle d'accès repose sur trois concepts: l'identification, l'authentification et l'autorisation.

L'identification revêt plusieurs significations:

- l'attribution d'un identifiant à une entité
- la détermination de l'identité d'une entité à partir de ses caractéristiques
- la communication par une entité de son identité. C'est cette dernière que nous retiendrons ici.

L'identification est une procédure de reconnaissance locale d'un acteur tandis que l'authentification est la reconnaissance de l'autre partenaire lors d'une communication à distance.

L'authentification peut alors consister en la vérification de l'identité d'une entité (logique, matérielle ou humaine) à partir d'une ou plusieurs de ses caractéristiques.

En fait, on ne peut admettre un bon niveau d'authentification que si le dispositif utilisé est sûr et nécessite la possession par l'entité d'un élément physique ou physiologique particulier.

L'autorisation donne un droit d'accès à une ressource, elle n'existe pas en tant que telle mais doit être déléguée par une autorité.

Le contrôle d'accès aux fichiers pour un utilisateur autorisé se fait par apposition sur chaque fichier d'une serrure logique ne s'ouvrant que pour certains utilisateurs et pour certains modes d'accès (lecture, création, modification, destruction). On utilise pour cela une matrice d'accès associant fichiers, utilisateurs et modes d'accès.

L'authentification des partenaires d'une communication peut se faire par emploi d'une procédure logicielle rendant difficile l'usurpation d'identité, procédure basée sur les techniques de cryptographie (III.C.6) et sur la carte à microprocesseur (III.C.7.a).

b. Les mesures destinées à sauvegarder l'intégrité

Son contrôle a pour vocation de garantir qu'une information (ou un ensemble d'informations) est telle qu'il doit être à un instant ou pendant une période donnée.

L'intégrité des messages est assurée lorsque seules les personnes habilitées ont pu l'émettre ou le modifier. Par modification, on entend aussi bien la modification du contenu que la modification de l'émetteur, du destinataire, la duplication ou le détournement. Notons au passage qu'une atteinte à l'intégrité implique dans la plupart des cas une atteinte à la confidentialité du message. Les diverses mesures à prendre sont, entre autres:

- prévenir la falsification d'enregistrements: l'intégrité d'un fichier doit être vérifiée
- authentifier l'information: le fichier doit être authentifié, la signature des messages échangés doit être authentifiée
- prévenir le rejeu
- les copies illicites des fichiers et des programmes doivent être évitées
- prévenir le vol d'information stockée

Le contrôle de l'intégrité d'un fichier est possible par utilisation d'un label d'intégrité recalculable.

L'authentification des messages échangés est possible grâce à la signature de ceux-ci: A envoie un message à B, B doit prouver que le message vient de A et A doit pouvoir prouver qu'il a écrit ou non le message. En cas de dispute entre les partenaires, il faut pouvoir prouver à une tierce personne que le message vient bien d'un expéditeur A et a bien été reçu par le destinataire B (en d'autres mots B doit pouvoir prouver que A l'a envoyé et A doit pouvoir le répudier s'il ne l'a pas effectivement envoyé). Ce problème sera traité lors de l'étude des signatures digitales (III.C.6.f.(3)).

Le rejeu est évité en ajoutant un élément supplémentaire tel un numéro de série ou un groupe date-heure.

c. Le chiffrement

Il doit assurer la confidentialité de l'information, c'est-à-dire tenir secrètes des informations pour ceux qui ne doivent pas en avoir connaissance. Il s'agit souvent de transformer un texte clair pour le rendre inintelligible aux personnes non autorisées. On utilise généralement un algorithme mathématique fonctionnant avec des clés secrètes ou publiques.

L'aspect confidentiel des informations ne peut véritablement être assuré que moyennant l'utilisation de techniques cryptographiques. Le chiffrement de messages est le seul moyen sûr pour doter les informations, lors de leur transfert d'un endroit sécurisé à un autre, de la confidentialité

exigée. Indiquons toutefois que le chiffrement, en tant que tel, n'est pas la solution idoine à tous les problèmes de sécurité des réseaux ! Il ne supprime pas la nécessité d'authentifier les interlocuteurs.

6. La cryptographie

a. Généralités

La cryptographie est une des techniques de protection de secrets les plus anciennes. Elle est extrêmement utilisée depuis que la majorité des systèmes d'information transportent l'information d'un lieu à un autre (les deux autres fonctions étant le traitement et le stockage). La cryptographie est en effet considérée comme le meilleur outil de protection.

La cryptographie sert aussi à authentifier un message, en prévenir l'altération et en certifier l'origine.

L'authentification est primordiale pour les applications bancaires (ou commerciales en général).

Le propriétaire du système est dépendant pour sa sécurité, en premier lieu, de l'intégrité de son fournisseur, qui dépend lui-même des développeurs et des mainteneurs du système. Lorsque le logiciel ou le système est en opération, des clés et des mots de passe sont introduits qui le protègent des ennemis extérieurs, y compris les ennemis fournisseurs. Dans ce cas la protection ne dépend que des opérateurs. Certains opérateurs occupent des places de haute importance tel celui qui charge le système avec les clés principales ou ceux qui transportent les clés d'une partie du système à l'autre. Une conception bien étudiée peut réduire le besoin de confiance de façon importante. Un contrôleur de sécurité peut par exemple être responsable pour l'application correcte de la procédure mais il n'est pas nécessaire qu'il connaisse la valeur des clés cryptographiques. De cette manière, la confiance étant placée en un certain nombre de personnes différentes, il y a peu d'opportunités pour un individu de corrompre le système entier.

Lorsqu'il y a un point particulièrement sensible, telle une clé principale de haut niveau, la responsabilité peut être partagée entre plusieurs individus avec pour conséquence qu'il faut collusion entre toutes ces personnes pour détruire la sécurité du système. En tous cas, il doit être facile de savoir en qui on place sa confiance et jusqu'à quel point.

b. Les chiffrements symétriques

(1) Schéma général du système de codage

Les éléments C et D représentent des organes de codage et de décodage: ils sont régis par des algorithmes qui à partir des deux variables à l'entrée donnent un certain résultat à la sortie.

Les deux entrées pour C sont:

- le texte en clair (ou le résultat d'un codage précédent) dénoté x
- la clé k

Le résultat est un texte codé y

Ce texte codé est une des entrées de D, l'autre étant de nouveau la clé k . Le résultat doit redonner x .

On notera: $y = C_k(x)$ et $x = D_k(y)$

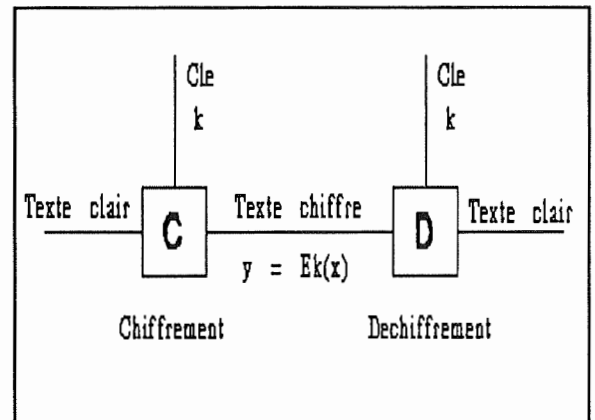


fig 1: Notations pour chiffrement et déchiffrement

(2) Utilité de la clé

La clé est essentielle dans le codage. En principe si la fonction $y = C(x)$ tenue secrète, elle peut servir à cacher x , mais si le secret de la fonction est connu, rien ne peut être tenté pour rendre sa valeur au codage. Une autre fonction est nécessaire. Etant donné que le développement et le test d'une nouvelle fonction est une lourde tâche, sa perte est très coûteuse. De plus, on doit avoir une confiance totale en ceux qui ont conçu, testé ou écrit les procédures de codage et de décodage. Le problème du secret est considérablement simplifié par l'emploi d'une clé qui n'est autre qu'un paramètre permettant la définition d'une large classe de fonctions de codage $y = C_k(x)$. Si une clé est découverte par l'ennemi, elle peut être changée et la fonction de codage reste valable.

Garder secrets la fonction ou algorithme $C_k(x)$ et la clé k est sage mais, considérant le nombre de personnes pouvant ou devant connaître sa forme, la fonction de codage ne peut être considérée comme fiable. C'est le secret de la clé qui importe. Le codage peut rester efficace même si l'ennemi connaît la fonction $C_k(x)$.

Lorsque $Ck(x)$ est une fonction standard (cas du Data Encryption Standard, III.C.6.c), n'importe qui peut la connaître.

(3) La distribution des clés

Lorsque le codage est employé pour sécuriser une communication, il doit y avoir accord préalable entre les différentes parties sur tous les aspects de la procédure. Un algorithme de codage, sa méthode d'utilisation et d'initialisation doivent être agréés.

L'exigence la plus difficile à remplir est que la clé doit être choisie et communiquée aux deux extrémités de la liaison. Avant que les données ne parcourent la liaison, la valeur de la clé doit en avoir fait de même. Des clés peuvent être codées en employant d'autres clés mais en dernier ressort une clé doit être distribuée de manière différente. Le codage ne doit pas dès lors être considéré comme une création de secret mais plutôt comme une extension du secret appliqué à la transmission de la clé à un plus grand volume de données codées avec cette clé. Lorsque le codage est employé pour protéger des données stockées, les manipulations sont plus faciles car le codage et le décodage se faisant dans un même lieu, la clé ne doit pas voyager mais elle est toujours aussi importante. Choisir les clés et les rendre accessibles aux seules personnes autorisées sont des aspects de la gestion des clés (key management). Après accord sur la méthode de codage, la gestion des clés devient la tâche majeure du concepteur de systèmes parce que la sécurité de tout le système est concentrée dans ces clés.

(4) Utilisation du codage

Le contenu d'un message est inconnu, sauf pour ceux sensés le recevoir qui, connaissant la clé, peuvent le décoder. La clé contrôle donc l'accès au contenu du message. Si le message codé est rendu public et que l'algorithme de codage est connu, la connaissance de la clé équivaut à l'accès au message. La connaissance de la clé permet de construire un autre message et dans les circonstances adéquates, un message peut être lu et écrit. L'utilisation de clés de chiffrement asymétrique rend possible le contrôle séparé de l'écriture et de la lecture.

Sans la connaissance de la clé, un ennemi ne peut modifier de façon utile un message. Il peut probablement altérer le message codé mais le message modifié lorsqu'il sera décodé contiendra des données aléatoires et farfelues car la non-connaissance de la clé empêche

l'ennemi d'avoir un contrôle sur la forme du message décodé. Sachant qu'un message contient certaines redondances, le message authentique produit à l'aide de la clé peut être distingué du message aléatoire. De cette manière son authenticité peut être prouvée à ceux qui connaissent la clé.

(5) Tables de codage

Les codes secrets (remplacement d'un mot ou groupe de mots par un autre suivant une table) ont tenu une grande place dans les techniques de cryptographie à usage général. Ils peuvent être rendus plus efficaces en s'assurant qu'à une entrée corresponde plusieurs sorties dans la table, c'est-à-dire que le code employé pour un mot ou groupe de mots n'est pas toujours le même mais est choisi aléatoirement parmi toutes les alternatives. De cette manière, un mot important revenant souvent ne sera pas trahi par la fréquence du code correspondant. Pour la protection de données informatiques, les codes sont loin d'être idéaux parce que la table de conversion doit être stockée et que la conversion elle-même peut demander beaucoup de temps. La génération d'une telle table de codes n'est pas des plus aisée. La protection de la table peut être difficile. Le transport rapide et sûr d'une table de codes au lieu où elle est nécessaire est d'autant plus difficile que les changements sont fréquents.

Les deux composants principaux des techniques de codage classiques sont la substitution et la transposition. Dans une substitution, les lettres sont remplacées par d'autres, dans une transposition les lettres sont arrangées dans un autre ordre. Le lecteur que l'évolution des codes à travers l'Histoire intéresse pourra consulter [DAV] 2.2 à 2.5.

(6) Les attaques contre les données codées

Avant l'avènement des ordinateurs, le décryptage dépendait uniquement de l'habileté humaine. C'était un art ésotérique requérant une intuition considérable de la part du pratiquant et une grande quantité de travail laborieux. Les ordinateurs ont changé cette situation. Pour toutes les méthodes classiques, l'analyse du texte codé pour identifier le type de chiffrement peut être menée rapidement.

Une fois que le mécanisme est connu, la vitesse de traitement des ordinateurs permet d'utiliser des méthodes grossières pour casser ces chiffrements classiques.

Dans la plupart des cas, la clé doit être trouvée avant que le message ne puisse être interprété. Une recherche exhaustive consiste à essayer toutes les valeurs possibles de la clé afin de voir laquelle convient. Trouver la clé par cette méthode peut représenter un travail énorme lorsque le nombre de valeurs possibles est grand. Très souvent, la connaissance de la clé est préférable à la possession d'un message décodé. Il est en effet courant que toute une série de message ait été encodé avec la même clé et tous les messages deviennent alors intelligibles.

(a) Les classes d'attaques

Lorsqu'on évalue les qualités d'un système de chiffrement, il est prudent de considérer que l'algorithme est connu du cryptanalyste et que la tentative de casser le message codé consiste simplement à essayer de trouver la clé.

La tâche de l'analyste est la plus difficile lorsqu'il n'a que le texte chiffré et aucune notion concernant le texte en clair (attaque "texte codé seul"). S'il n'y a pas de redondance dans le texte en clair (par exemple une chaîne de nombre arbitraire) alors il est impossible de trouver la clé: pour un texte codé donné chaque valeur de la clé donne comme texte clair une chaîne arbitraire et toutes ces chaînes sont équiprobables. La connaissance du texte clair peut résoudre ce problème, par exemple si le message arbitraire a un entête dans un format standard. Si l'entête est suffisamment long, il permet d'identifier la clé avec certitude étant donné que cet entête n'apparaît que pour une seule valeur de la clé. Si l'entête est trop court, on peut toutefois réduire l'ensemble des clés possibles.

Dans la seconde classe d'attaques, le cryptanalyste connaît certains textes codés et les textes en clair correspondants (attaque "texte en clair connu"). Le travail consiste alors à trouver une clé faisant correspondre les deux textes. Si la longueur du texte disponible est suffisante, la clé peut être identifiée avec certitude. Les cas où le texte en clair et le texte chiffré sont connus sont assez fréquents. Par exemple des changements du marché peuvent conduire à l'envoi d'instructions prévisibles d'un banquier à un autre.

Dans la troisième classe d'attaques, la plus favorable pour le cryptanalyste, le texte en clair est choisi (attaque "texte en clair choisi"). Le crypt-

analyste demande à un complice d'introduire un texte en clair de son choix dans le processus de chiffrement. Le texte en clair peut être choisi pour faciliter la tâche de recherche de la clé (un texte composé de tous zéros par exemple). Un mot probable est un exemple de texte en clair connu, même si sa position dans le texte est inconnue du cryptanalyste. Une des tentatives anglaises pour casser le procédé Enigma des Allemands lors de la Seconde Guerre mondiale fut de les obliger à rédiger un message contenant un mot bien précis.

Afin d'évaluer les qualités d'un chiffrement, il est recommandé d'utiliser les hypothèses les plus défavorables concernant l'information disponible pour l'ennemi. En pratique, l'hypothèse la plus employée est que l'algorithme de chiffrement est connu, ainsi qu'une quantité suffisante de texte clair et de texte codé correspondant pour déterminer la clé. En d'autres mots, une attaque avec texte en clair connu est possible. Une hypothèse plus sévère consiste à prévoir une attaque avec texte en clair choisi. Si la méthode d'attaque consiste en une recherche exhaustive de la clé en utilisant un ordinateur étant donné un couple texte en clair texte chiffré connu, on peut estimer le temps moyen nécessaire pour trouver la clé en partant du temps nécessaire à tester une clé et du nombre de clés différentes possibles. La possibilité de tester plusieurs clés en parallèle doit également être prise en compte.

(7) Le chiffrement en continu

Lorsqu'un système de communication requiert le traitement de caractères en continu, chaque caractère doit être accepté dès qu'il est disponible, codé et ensuite transmis. Certaines formes de substitution sont permises mais un chiffrement avec transposition ne l'est pas. Les données du texte en clair arrivant de cette manière sont traités par ce que l'on appelle un chiffrement en continu.

(a) Le chiffrement de Vernam

Ce chiffrement consiste en la combinaison bit par bit de caractères aléatoires avec les caractères du texte en clair, la combinaison étant l'addition modulo 2 (en fait la fonction XOR). Le déchiffrement est alors très simple:

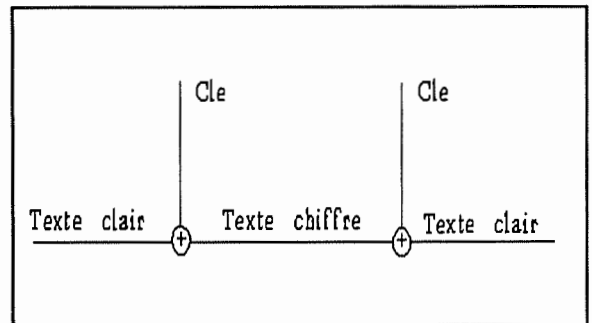


fig 2: Le chiffrement de Vernam

il suffit de recommencer la même opération d'addition modulo 2 avec une copie de la série de caractères aléatoires. Il est à remarquer que si la clé est inconnue, ce système est inattaquable car pour un texte codé donné avec une clé aléatoire inconnue, tous les textes en clair possibles de même longueur sont équiprobables. Il est cependant nécessaire de donner à l'émetteur et au récepteur la série composant la clé. Etant donné que la clé doit avoir une longueur égale à celle du message, ce système est peu employé, mais il est des situations requérant un haut degré de sécurité et où les quantités d'informations sont petites mais doivent être communiquées d'urgence et de plus le transport des clés n'est pas difficile. Cette méthode est connue sous le nom de one-time-tape et est notamment utilisée pour la protection du téléphone rouge entre Washington et Moscou.

(8) Le chiffrement par blocs

Le chiffrement par blocs traite le texte en clair en le découpant en blocs de longueurs égales et en chiffrant chaque bloc indépendamment. La taille du bloc dépend de l'appareil de chiffrement utilisé. Le DES (Data Encryption Standard, III.C.6.c) utilise des blocs de 64 bits. Le chiffrement par blocs est plus rapide que le chiffrement continu. Les données peuvent être efficacement traitées dans des applications telles le transfert de fichiers. Mais étant donné qu'il n'y a pas d'influence des autres blocs sur le chiffrement d'un bloc particulier, cette méthode présente des désavantages:

- si un bloc apparaît plusieurs fois dans le texte en clair, le texte codé correspondant sera également répété donnant ainsi une information à l'ennemi.

- l'ennemi peut changer l'ordre des blocs sans être découvert.

Les désavantages de cette méthode sont réduits au fur et à mesure de l'utilisation de blocs de plus grande longueur.

(9) Mesure de la qualité d'un chiffrement

Shannon a identifié deux classes différentes de systèmes de codage: ceux qui sont sûrs inconditionnellement et ceux qui sont sûrs numériquement. Un système est sûr inconditionnellement s'il est incassable même si le cryptanalyste a une puissance de calcul infinie à sa disposition. Le seul système sûr inconditionnellement couramment utilisé est le système one-time-tape utilisé avec une clé complètement aléatoire.

Un cryptogramme particulier peut être sûr inconditionnellement s'il est trop court, ne contenant pas assez d'informations pour conduire à une solution unique. Même un chiffrement par substitution monoalphabétique peut tomber dans ces conditions.

Un texte codé est appelé sûr numériquement si la recherche de la solution est tellement fastidieuse qu'elle est impossible à réaliser dans un délai raisonnable avec la puissance de calcul réaliste la plus grande. Les fonctions unidirectionnelles (III.C.6.f.(2)(a)) tombent dans cette catégorie. Il n'y a pas de définition précise de ce qui est numériquement réalisable étant donné que des ordinateurs de plus en plus rapides peuvent être employés et peut être en grand nombre. On considère actuellement que cette limite est de 10^{25} états.

La longueur de la clé et son effet sur le temps de recherche exhaustive fixe une limite supérieure pour la qualité du chiffrement mais c'est une erreur de se contenter de cette estimation. L'histoire est remplie de chiffrements inattaquables avec des espaces de clés énormes. La recherche exhaustive n'est qu'une méthode universelle que l'on utilise lorsque toutes les autres ont échoué. La qualité d'un chiffrement est une caractéristique négative et dépend de la maladresse de l'ennemi à trouver la méthode pour le découvrir. Elle ne peut jamais être garantie excepté pour les chiffrements inconditionnellement sûrs.

(10) Menaces contre les systèmes protégés

Les menaces contre les systèmes protégés qu'ils soient des systèmes de communication ou des systèmes de stockage des données, peuvent être classifiées en deux catégories: les menaces actives et les menaces passives.

Une attaque passive est simplement une tentative de contournement des protections et de lecture de ce qui est transféré ou stocké mais sans altération des données. Avant l'introduction

du multiplexage, il était très simple de mettre une ligne de transmission sur écoute. Les formes variées de multiplexage et les protocoles complexes dans les réseaux de communication de données demandent une plus grande sophistication à l'ennemi mais cela reste toujours à sa portée. Une mesure précise des caractéristiques de la ligne permet parfois de détecter une écoute lorsqu'il s'agit d'une liaison physique mais cela est impossible lorsqu'une liaison micro-ondes est utilisée. La défense contre l'écoute passive doit donc être basée sur le chiffrement des données transmises. On ne peut se fier à une protection de la ligne de transmission seule, excepté si la ligne est totalement protégée physiquement ce qui est très rare en pratique.

La menace active est potentiellement de loin plus sérieuse. Dans ce cas l'intrus tente d'altérer les données transmises ou stockées et espère le faire sans être découvert par le détenteur légitime ou l'utilisateur des données. L'utilisation du chiffrement peut protéger les données contre une altération en les arrangeant de telle sorte qu'une altération ayant un sens ne peut être faite sans chiffrer le message. Lorsqu'un intrus obtient un accès illégal aux supports de stockage des données, la destruction des données ne peut être empêchée. Il faut donc un environnement physique sécurisé pour le stockage des supports ainsi que des copies de sauvegarde rangées en d'autres lieux.

Réussir une intrusion active avec succès n'est pas simple. La communication entre la source et le destinataire

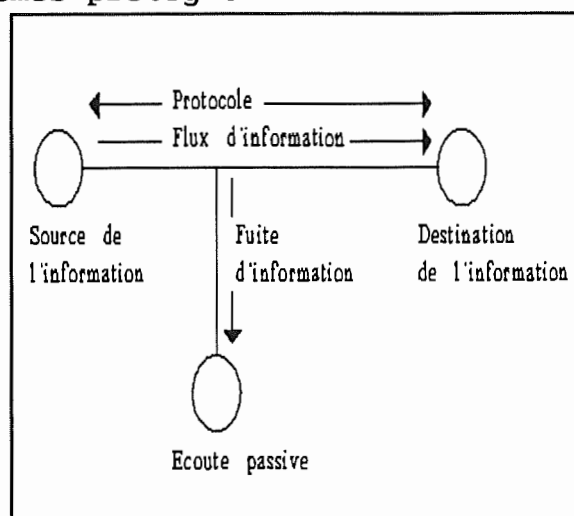


fig 3: Schéma de principe d'une écoute passive

re est contrôlée par un protocole (appelé vrai protocole sur la fig 3). L'intrus doit interrompre ce protocole et générer un faux protocole avec la source et avec le destinataire, leur faisant croire à tous deux qu'ils sont toujours en communication directe. L'information vraie va de la source vers l'intrus. L'information fausse va de l'intrus vers le destinataire. La tâche de l'intrus est plus simple s'il s'introduit dans le circuit au début de la communication plutôt que lorsqu'elle est déjà entamée. Avec certains artifices, l'intrus peut prendre part au processus de mise en place du canal.

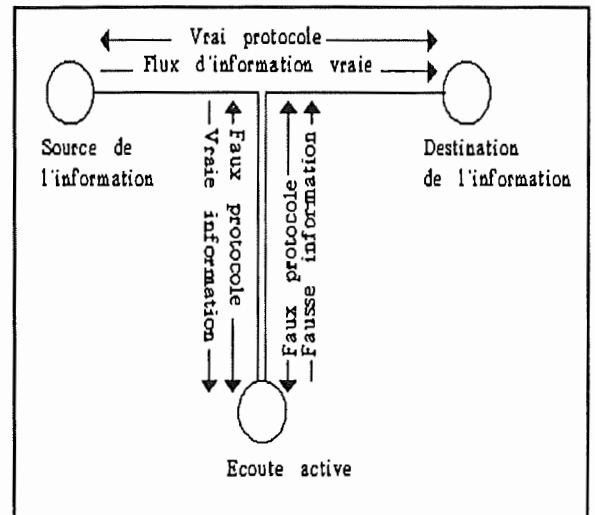


fig 4: Schéma de principe d'une écoute active

(11) Le rejeu

Il est nécessaire d'empêcher une altération non détectée, une addition, une destruction d'une partie du message ou un rejeu. Le rejeu est une attaque où l'intrus enregistre une partie codée et la réinjecte ensuite à partir de son point d'écoute. Le rejeu ne peut être empêché mais il peut être détecté en incluant dans le message en clair un bloc identificateur contenant soit un numéro de série ou si possible une indication du temps. Le récepteur ignore alors tout message codé lorsque le texte en clair ne contient pas les indications valides.

(12) La clé de chiffrement

Dans la pratique, les sécurités des systèmes de chiffrement ne dépendent pas du secret de l'algorithme mais bien du secret des clés de chiffrement. Ce principe entraîne une responsabilité considérable du développeur du système générant les clés, les distribuant, les utilisant et les détruisant après usage. Dans le passé les clés étaient envoyées aux utilisateurs par des courriers humains mais cette façon de procéder est trop lente et trop peu pratique pour la plupart des applications actuelles. Dès lors on a tenté de transporter les clés plus rapidement et plus efficacement. Ce qui implique souvent leur envoi via le canal de communication qui est lui-même l'objet de la protection chiffrée. Nous avons donc besoin d'une hiérarchie de clés qui distingue celle utilisée pour la protection des données et qui sont donc beaucoup plus employées, de celles utilisées uniquement pour la protection des clés en transit. Les clés utilisées pour le codage des autres clés sont utilisées beaucoup moins fréquemment et peuvent être transportées par des moyens beaucoup moins efficaces, une visite physique, par exemple. Le fait qu'elles sont utilisées moins fréquemment signifie qu'elles sont moins exposées à une attaque.

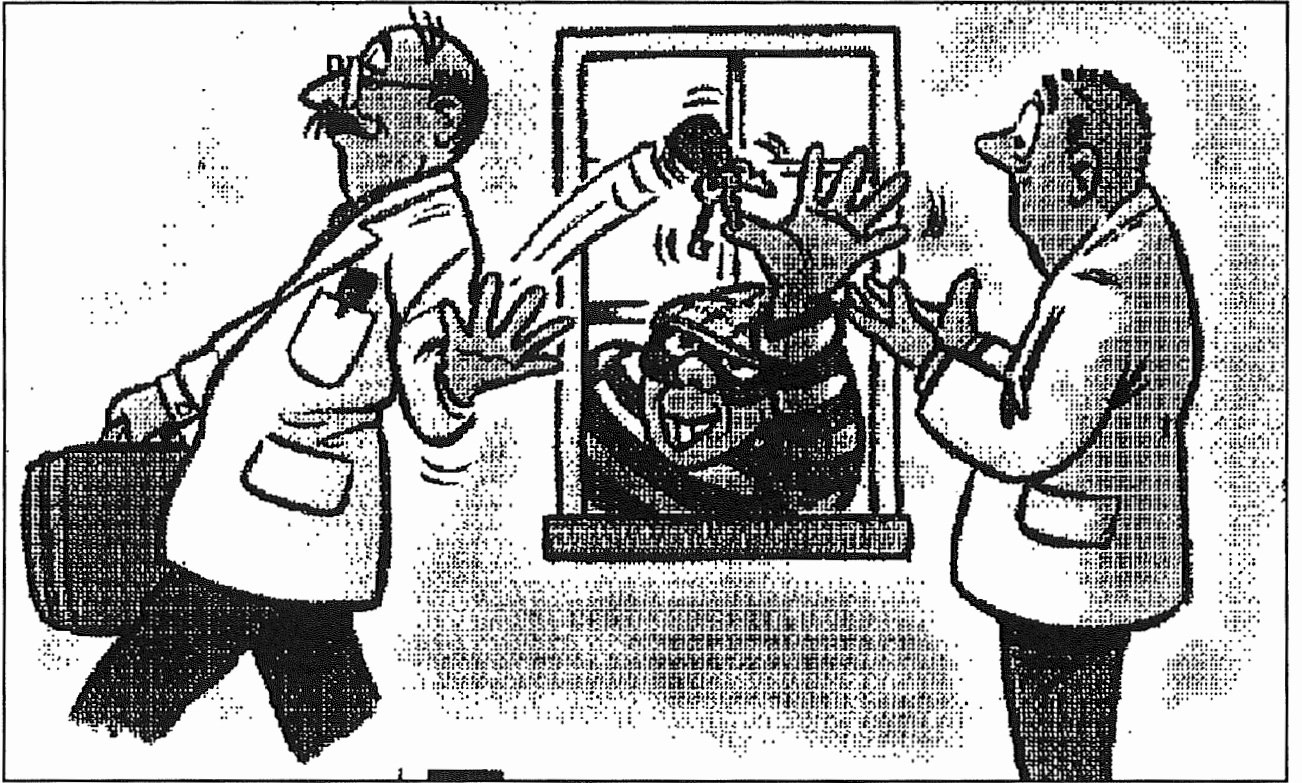


fig 5

c. Le Data Encryption Standard

(1) Histoire

Pourquoi a-t-on besoin d'un standard alors que des systèmes de chiffrement sont disponibles chez plusieurs fournisseurs ? Un utilisateur voulant protéger ses communications a simplement besoin d'une paire d'appareils de chiffrement compatibles et de clés correspondantes. Il est ainsi prêt à communiquer en toute sécurité.

Tant que la communication reste interne à un groupe particulier, la protection de la communication par chiffrement ne requiert qu'un accord sur une méthode particulière de codage. Jusqu'à présent, la plupart des communications de données se faisaient à l'intérieur d'organisations souvent à l'aide d'un réseau privé de lignes louées. Dans ces conditions, un standard n'est pas nécessaire.

Lorsque des communications protégées sont nécessaires entre des utilisateurs appartenant à différentes organisations, l'accord est moins facile à trouver. Ces organisations peuvent avoir choisi des appareils de chiffrement de différents fournisseurs et dans ce cas il est fort probable qu'ils soient totalement incompatibles et incapables de communiquer entre eux. Afin de rendre l'interfaçage possible l'algorithme de chiffrement doit être conforme à un standard et doit donc être public alors que la tendance habituelle était de garder cet algorithme secret.

(2) Caractéristiques

La protection d'un système basé sur un standard public doit reposer sur la puissance de l'algorithme et le secret de la clé de chiffrement. Un tel algorithme standard doit:

- fournir un haut degré de sécurité
- être complètement spécifié et aisé à comprendre
- la sécurité fournie par l'algorithme ne doit pas être basée sur le secret de cet algorithme
- il doit être disponible pour tous les utilisateurs et fournisseurs
- il doit être adaptable pour une utilisation dans diverses applications
- il doit être économique à implanter et efficace à l'usage
- il doit pouvoir être validé

Les chiffrements par substitution ou les chiffrements par

transposition utilisés seuls sont très faibles. Cependant des opérations de chiffrement intrinsèquement faibles peuvent être combinées pour former un système plus puissant. Le chiffrement ainsi constitué est appelé chiffrement produit.

Un chiffrement produit reçoit un bloc de texte en clair, transpose l'ordre des bits (diffusion) et ensuite effectue une substitution en accord avec une table (confusion). Ces deux étapes peuvent être répétées plusieurs fois.

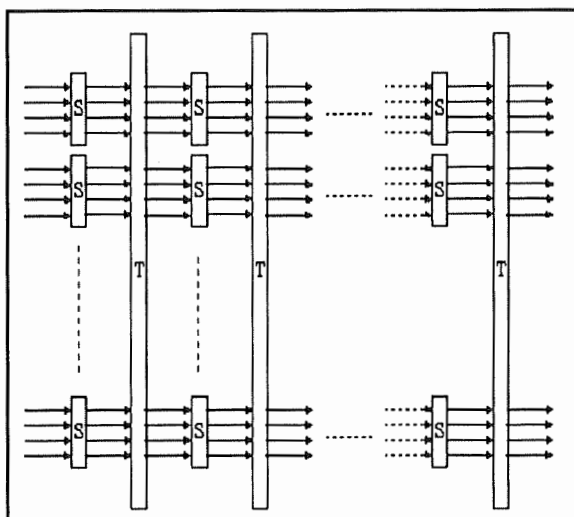
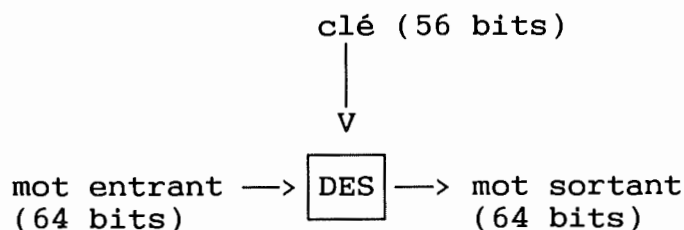


fig 6: Exemple de chiffrement produit

Le DES est un exemple de ces chiffrements produit.

(3) Description sommaire du DES

L'algorithme DES travaille sur des mots de 64 bits. La clé utilisée est de 56 bits + 8 bits de parité.



La structure logique du DES est assez complexe. Le mot à coder est présenté à l'entrée INPUT et le mot codé sortira à la sortie OUTPUT (64 bits tous deux). La clé est introduite à la porte KEY et, après retrait des 8 bits de redondance, traitée de façon particulière par un générateur de clés secondaires. Le mot à coder parcourt la boucle (grossoière approximation: le lecteur intéressé peut consulter [DAV]) registre R, permutation-expansion E, opération ou-exclusif avec la clé secondaire, boîtiers de substitutions S, permutation P, opération ou-exclusif avec le registre L (dépendant d'une partie du mot en entrée de boucle). Cette boucle est répétée seize fois, la clé secondaire utilisée changeant à chaque

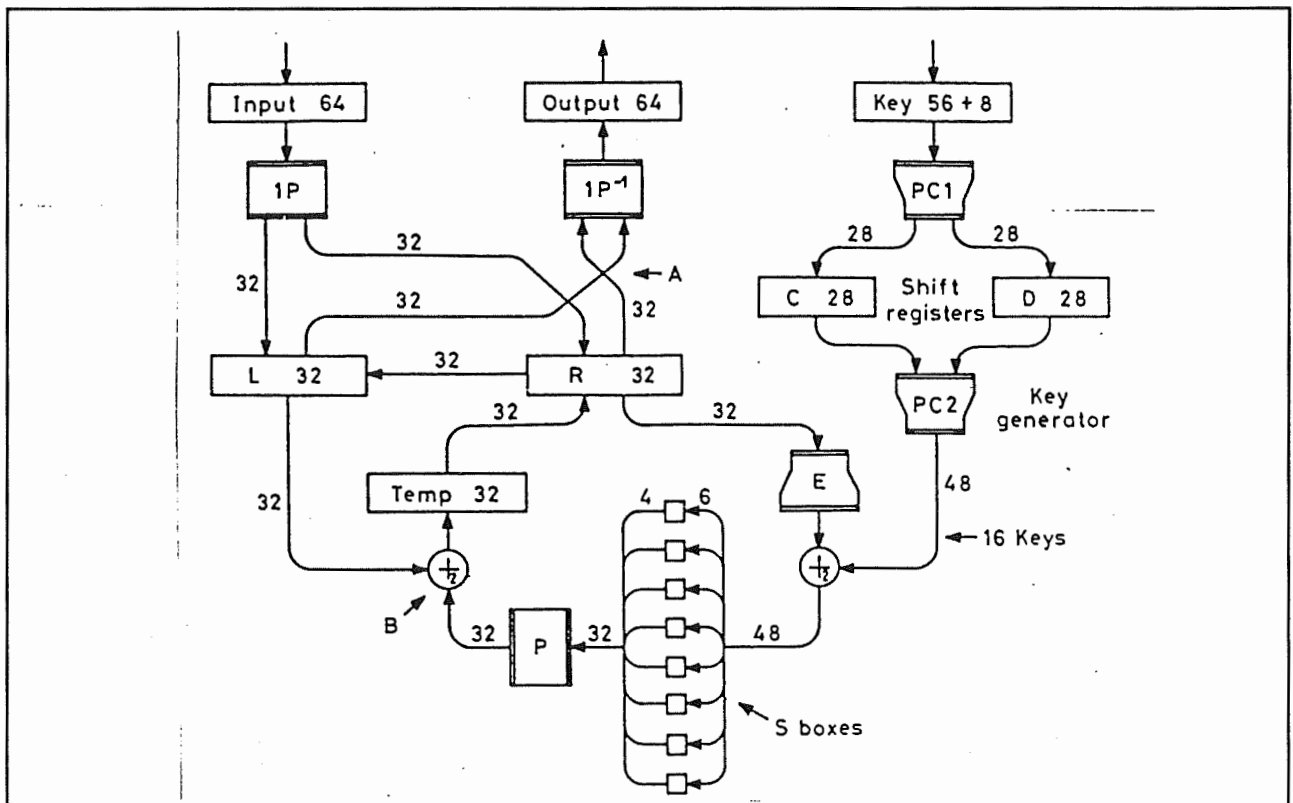


fig 7: Structure logique du DES

itération.

On peut montrer par quelques exemples qu'un changement d'un bit dans le texte en clair ou dans la clé entraîne de nombreux changements dans le texte codé (idéalement changement de tous les bits avec une probabilité $1/2$) rendant quasiment impossible la recherche d'une corrélation entre texte en clair et texte codé.

Le DES était certifié jusqu'en 1988, la NSA (National Security Agency) estimant son "cassage" possible après cette date. Une étude de la solidité de l'algorithme est faite en [SMI].

De nouveaux standards de chiffrement seront nécessaires si les standards actuels sont jugés inadéquats parce que les moyens technologiques pour les attaques sont devenus plus performants. On peut développer un algorithme plus performant simplement en étendant l'espace des clés du DES. Si on désire le faire on doit également examiner les paramètres internes, c'est-à-dire la structure des transpositions et substitutions et le nombre de boucles auxquelles les données sont assujetties.

Si la structure générale de l'algorithme DES est maintenue, les paramètres qui peuvent être changés sont la taille du bloc de données, la taille de la clé, le générateur des sous-clés, la méthode d'utilisation de la clé, les permutations et les boîtiers de substitution. Il est sans doute souhaitable de retenir des blocs de données de 64 bits afin de ne pas devoir modifier l'algorithme. Une complexité légèrement plus grande du générateur de clés peut s'avérer nécessaire pour éviter le plus possible le choix de mauvaises clés.

d. Utilisation du chiffrement par blocs en pratique

(1) Les méthodes

Il existe quatre méthodes d'utilisation du chiffrement par blocs:

- l'Electronic CodeBook (ECB) qui est l'utilisation directe de l'algorithme de chiffrement pour un bloc
- le Cipher Block Chaining (CBC) qui est l'utilisation répétée de l'algorithme pour coder un message constitué de plusieurs blocs en faisant dépendre le codage du bloc courant des blocs précédents
- le Cipher Feedback (CFB) qui est l'utilisation de l'algorithme pour encoder des caractères en continu, traitant chaque caractère dès son arrivée.

Le premier mode est appelé Electronic Codebook (Livre de Codage Electronique) parce que pour une clé donnée, il associe à chaque valeur d'un bloc en entrée une valeur unique d'un bloc en sortie et vice-versa. A cause du grand nombre de telles valeurs (2^{64}) le livre de codes en question est très grand, pratiquement impossible à énumérer complètement.

D'autres méthodes d'utilisation sont possibles mais les trois ci-dessus résolvent la plupart des problèmes. Elles sont définies dans un document, le Federal Information Processing Standard et sont sur le point de devenir des standards internationaux. Ces trois méthodes peuvent être utilisées avec n'importe quel chiffrement par blocs.

(2) Les limitations du mode Electronic Codebook

On pourrait penser que pour chiffrer un message contenant plusieurs blocs il suffit de le diviser en blocs de 64 bits et de les coder séparément. Ce serait alors une simple application du chiffrement ECB.

Mais cette méthode présente des faiblesses très grandes qui sont dues à la structure des messages typiques. Dans

toutes les applications pratiques, des fragments de messages ont tendance à être répétés. Un message peut avoir des séquences communes avec un autre. Les messages générés par ordinateur ont leur propre type de structure. Le besoin de définition formelle des protocoles et le souci de généralité dans leur définition fait que des formats identiques sont souvent répétés. Si elles sont situées identiquement par rapport aux frontières de bloc, des phrases répétées seront détectées comme telles, après être passées dans le chiffrement ECB. Le plus grand danger se produit lorsque des parties significatives du message changent peu et apparaissent à des places fixes. La faiblesse de la méthode ECB est due au fait qu'il n'y a aucune connexion des blocs entre eux.

En codant chaque bloc séparément, on laisse des parties totalement indépendantes que le cryptanalyste peut analyser et assembler à son propre bénéfice. Ce dont nous avons besoin c'est d'une méthode de codage de blocs successifs qui rend le texte codé sans signification excepté dans la séquence donnée. C'est ce que l'on appelle le chiffrement par chaînage.

(3) Chiffrement par chaînage de blocs

(a) Principe

Le chiffrement par chaînage de blocs utilise la sortie d'une étape de chiffrement pour modifier l'entrée de la suivante. Ainsi chaque bloc chiffré est dépendant non seulement du bloc de texte en clair dont il provient mais également de tous les blocs en clairs précédents. Cette méthode est illustrée à la fig 8.

Toutes les opérations y fonctionnent en 64 bits en parallèle. L'opération d'addition est en fait l'opérateur ou exclusif XOR et opère en parallèle sur les 64 bits des blocs. Le mode d'opération CBC est caractérisé par une rétroaction du texte chiffré à l'entrée de l'émetteur et une action symétrique du texte chiffré à la sortie

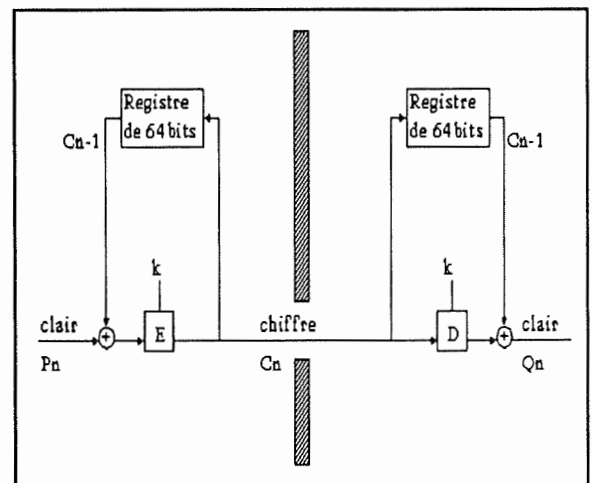


fig 8: Chiffrement par chaînage de blocs

du récepteur.

A l'exception du premier bloc, chaque bloc avant chiffrement est "additionné" au texte codé du bloc précédent ce qui rend le texte codé du bloc C_n fonction de tous les blocs en clair P_1 à P_n . La partie droite de la figure illustre le décodage. Après décodage du texte codé, une correction est apportée qui correspond exactement à la même opération effectuée au début (le ou exclusif) avec le bloc de texte chiffré précédent.

Pour le chiffrement on a :

$$C_n = Ek(P_n \text{ XOR } C_{n-1})$$

et pour le déchiffrement

$$Q_n = Dk(C_n) \text{ XOR } C_{n-1}$$

Après application de l'opérateur Dk à la première équation :

$$Dk(C_n) = P_n \text{ XOR } C_{n-1}$$

et par substitution de cette valeur dans la seconde équation

$$Q_n = P_n \text{ XOR } C_{n-1} \text{ XOR } C_{n-1} = P_n$$

ce qui montre bien que le texte décodé est la copie du texte à l'entrée.

Pour compléter la définition de l'opération CBC, le départ et la fin de la procédure doivent être spécifiés. Au début le texte codé précédent n'est pas disponible. Le contenu initial du registre doit donc être spécifié. Nous l'appellerons I , variable d'initialisation ou vecteur d'initialisation. Le choix de cette valeur est important pour la sécurité et doit être le même pour l'émetteur et pour le récepteur. Les équations de codage et décodage doivent être remplacées pour $n=1$ par

$$C_1 = Ek(P_1 \text{ XOR } I)$$

$$Q_1 = Dk(C_1) \text{ XOR } I$$

Les équations données plus haut restant valables pour $n > 1$.

La fin du message doit être allongée afin de donner

un multiple de 64. Elle peut être complétée en ajoutant des zéros par exemple car l'addition avec le texte codé précédent la protège d'une analyse du type livre de codage (méthode précédente)

(b) Les erreurs de transmission dans le chiffrement CBC

La boucle de rétroaction étend indéfiniment l'effet de tout changement à l'entrée de telle sorte qu'une simple erreur d'un bit dans le message en clair affecte le texte chiffré à partir du bloc où l'erreur se produit et influence également tous les blocs de texte chiffrés suivants. Cela n'est pas aussi important que ce que l'on pourrait craindre car le processus de déchiffrement redonne le texte en clair correct excepté pour le bit erroné.

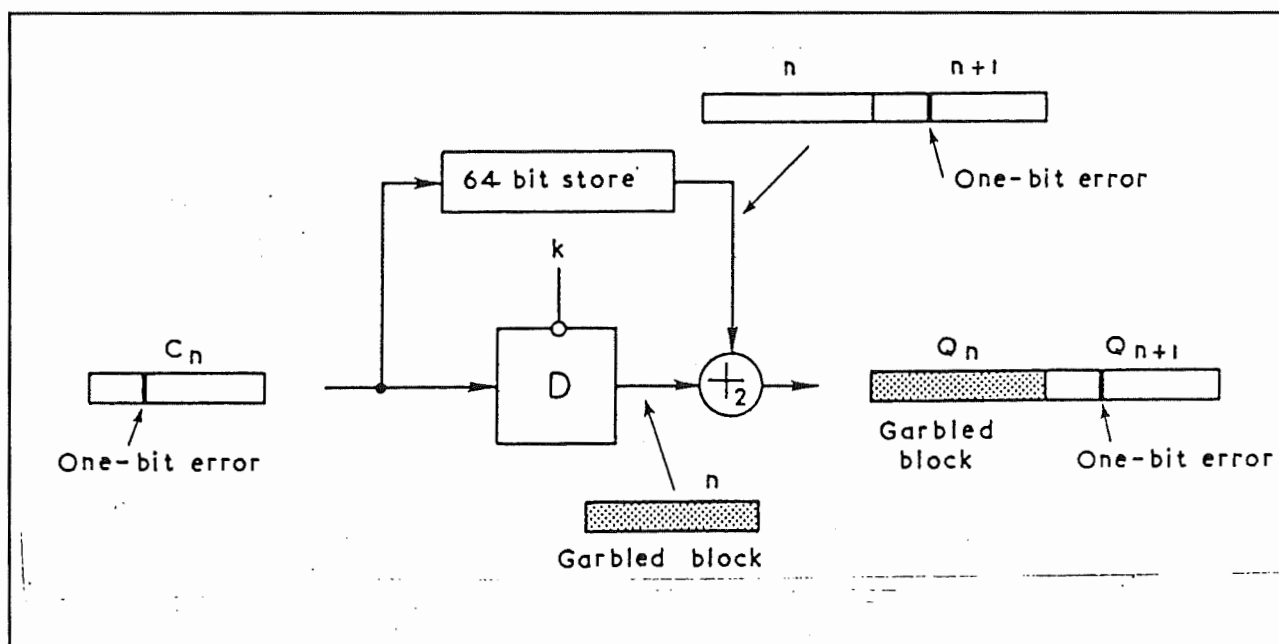


fig 9: Erreur d'un seul bit (méthode CBC)

Des erreurs dans le texte chiffré sont plus importantes. Elles résultent par exemple d'une liaison bruyante ou d'un mal fonctionnement du support de stockage. L'effet d'une erreur d'un seul bit dans le texte chiffré est illustré à la fig 9. Le premier effet est de changer l'entrée de l'algorithme DES au récepteur. La sortie de l'algorithme est alors aléatoire à cause des propriétés de chiffrement de l'algorithme. Lors du traitement du bloc suivant, l'erreur dans le texte chiffré se propage du registre de droite vers l'entrée de l'organe de déchiffrement et une erreur d'un seul bit dans ce texte chiffré

cause une erreur d'un seul bit dans le texte en clair, à la position correspondante dans le second bloc. Les blocs après le second ne sont pas affectés par l'erreur dans le texte chiffré.

Le chaînage par blocs de chiffrement est donc une procédure autocorrectrice. Deux blocs du texte en clair à la sortie seront affectés mais le système continuera à fonctionner correctement par après.

Une perte de synchronisation est beaucoup plus grave. Il est possible qu'un bit soit perdu ou qu'un bit soit introduit dans la transmission et de ce fait les blocs seront décalés d'une position vers la gauche ou vers la droite et le système de réception générera des données incompréhensibles indéfiniment. L'utilisation de protocoles spéciaux peut empêcher cette perte de synchronisation.

e. Distribution des clés

	Connu de X	Public	Connu de Y
Initialement	x	a, p	y
Echange	a^x	a^x, a^y	a^y
	a^y		a^x
Calcul	$(a^y)^x$ $= a^{xy}$		$(a^x)^y$ $= a^{xy}$

tableau 2: Distribution de clés par fonction exponentielle

Il est possible de distribuer des clés secrètes grâce à des échanges de messages qui ne sont pas secrets. Le principe de la méthode est le suivant:

- les deux parties X et Y choisissent un grand nombre premier p et un générateur pour l'arithmétique modulo p . La notion de générateur est explicitée en [DAV] chapitre 8. Retenons ici qu'il s'agit d'un nombre $a < p$ tel qu'il existe une bijection

$$\begin{aligned} \{0, 1, \dots, p-2\} &\longrightarrow \{1, 2, \dots, p-1\} \\ x &\longrightarrow a^x \text{ modulo } p \end{aligned}$$

Dans le tableau ci-dessous, les générateurs possibles sont: 1, 3, 7 et 9.

Ce nombre premier p doit être tel que la fonction a^x modulo p soit facilement calculable (ce qui est toujours le cas) mais que son inverse soit difficilement calculable.

Les nombres p et a sont rendus publics. Chacune des parties choisit également un nombre secret entre 0 et $p-1$, respectivement x et y , et calcule a^x et a^y qu'ils s'échangent les rendant ainsi publics. Enfin chaque partie calcule respectivement $(a^x)^y$ et $(a^y)^x$ qui sont évidemment égaux et qui ne sont connus que de X et Y . Ce nombre a^{xy} peut être utilisé comme clé secrète.

Le grand défaut de cette méthode est qu'elle requiert l'authentification préalable des deux parties.

x

	1	2	3	4	5	6	7	8	9	10
0	1	1	1	1	1	1	1	1	1	1
1	1	2	3	4	5	6	7	8	9	10
2	1	4	9	5	3	3	5	9	4	1
3	1	8	5	9	4	7	2	6	3	10
4	1	5	4	3	9	9	3	4	5	1
5	1	10	1	1	1	10	10	10	1	10
6	1	9	3	4	5	5	4	3	9	1
7	1	7	9	5	3	8	6	2	4	10
8	1	3	5	9	4	4	9	5	3	1
9	1	6	4	3	9	2	8	7	5	10
-	-	-	-	-	-	-	-	-	-	-
10	1	1	1	1	1	1	1	1	1	1
11	1	2	3	4	5	6	7	8	9	10

tableau 3: Table des puissances et exponentielles modulo 11

f. Les chiffrements asymétriques (à clé publique)

La plupart des systèmes cryptographiques emploient des chiffrements symétriques: la clé secrète unique est connue de l'expéditeur et du destinataire. Rien ne les distingue et ce système permet une communication dans les deux sens. En 1976 est apparu un nouveau système dans lequel l'expéditeur et le destinataire emploient des clés différentes. Seule la clé du destinataire est gardée secrète, la clé de l'émetteur pouvant être publiée sans affaiblir le système. Ce système asymétrique ne permet la communication que dans un seul sens. Son

grand avantage est qu'il élimine le besoin de transporter une clé entre le destinataire et l'expéditeur. La réduction du nombre d'endroits où la clé doit être maintenue secrète améliore également la sécurité.

(1) Principe

Le chiffrement se fait grâce à l'algorithme E et la clé k_E , le déchiffrement grâce à l'algorithme D et la clé k_D . E et D sont connus et constants, k_D est secret et k_E connu. Une nouvelle paire k_E, k_D peut être générée chaque fois que nécessaire.

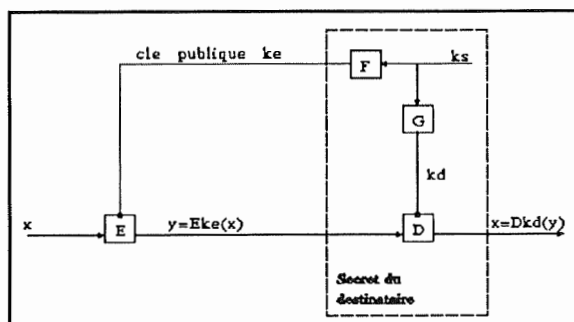


fig 10: Principe du chiffrement à clé publique

Pour que k_D permette le déchiffrement, elle doit évidemment être reliée à k_E par une relation particulière. La génération des clés se fait par celui qui détiendra la clé secrète. Le trait pointillé indique l'espace à sécuriser.

La clé de l'émetteur étant publique, aucune authentification n'est possible. L'emploi de signatures digitales permet de remédier à cet inconvénient:

- A et B produisent chacun une clé publique k_A et k_B
- A et B connaissent la clé publique de l'autre
- A écrit un message pour B contenant un nombre aléatoire R et codé avec la clé publique de B
- Seul B peut décoder le message et il renvoie R dans sa réponse codée avec la clé publique de A
- A peut décoder la réponse et vérifie que le R correct y est présent
- A considère alors que le message vient bien de B

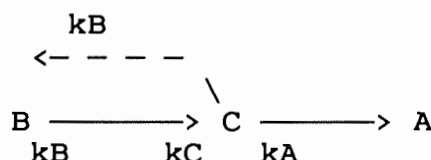
La procédure symétrique permet une authentification réciproque.

Les chiffrements asymétriques à clés publiques souffrent de quelques faiblesses:

- l'ennemi, s'il a quelques indices sur la forme du message, peut coder un message-test (avec la clé publique)

et comparer le résultat avec le message codé venant de l'émetteur. La probabilité de trouver le bon message peut alors être élevée.

- il faut être certain de la clé publique de l'émetteur. Un ennemi C pourrait transmettre une clé publique à B (k_B). B enverrait des messages que C pourrait décoder (grâce à sa clé secrète k_C associée à k_B) et renvoyer vers A grâce à la connaissance de la clé publique de A (k_A).



(2) Construction d'un système à clés publiques

(a) Le principe

L'algorithme le plus connu est le RSA du nom de ses promoteurs Rivest, Shamir et Adleman. La fonction E et la clé k_E étant connues, le texte codé y est une fonction connue du texte en clair x . Il doit être impossible de calculer x en fonction de y ce qui implique que la fonction E (chiffrement) doit être une fonction unidirectionnelle (pas d'inverse). La fonction de génération de la clé k_E doit aussi être unidirectionnelle. Cela peut paraître paradoxal car l'inverse de E c'est précisément D . Par unidirectionnel, on veut exprimer le fait que sans la connaissance de k_D , la fonction E n'est pas invertible mais la clé k_D est une sorte de trappe dont la connaissance rend facile l'inversion de E .

(b) La fonction puissance

Soit la fonction $y = x^m \text{ modulo } p$. On peut montrer (théorème de Fermat) que si $mn = 1 \text{ modulo } (p-1)$ et $y = x^m$ alors $x = y^n \text{ modulo } p$ (fonction inverse). Pour que la fonction inverse existe, il faut que m et n n'aient pas de facteur commun avec $p-1$ (si n est premier avec $p-1$, il existe m tel que $mn = 1 \text{ modulo } (p-1)$, m est d'ailleurs aussi premier avec $p-1$). Trouver m à partir de n est facile mais si aucun des deux facteurs n'est connu, la recherche peut être très difficile (recherche de facteurs d'un nombre). Cette propriété est exploitée dans le RSA.

(c) Chiffrement sans transport de clés

Il est possible de chiffrer des messages sans qu'il soit nécessaire de transporter les clés. La méthode est la suivante: M dispose d'une paire m, n et U d'une paire u, v satisfaisant toutes deux les conditions du III.C.6.f.(2)(b). M code le message: $X \rightarrow X^m$ et l'envoie à U. U le code à son tour grâce à u : $X^m \rightarrow X^{mu}$ et le renvoie à M qui retire son codage grâce à n : $X^{mu} \rightarrow X^{mun} = X^u$. Le message est renvoyé vers U qui le décode: $X^u \rightarrow X^{uv} = X$.

A nouveau, le gros défaut de cette méthode est le besoin d'authentification.

(d) L'algorithme RSA

Le RSA tire sa puissance de la complexité de résolution du problème de factorisation d'un nombre alors que l'opération inverse, la multiplication de deux nombres, est très facile à effectuer. Le défaut principal du RSA par rapport au DES est sa relative lenteur. L'algorithme est décrit en [RIV] et [DAV].

Les algorithmes à clés publiques utilisent deux clés:

- une clé de chiffrement PK connue de tous
- une clé de déchiffrement SK gardée secrète

Tout le monde peut chiffrer un message avec la clé PK mais seuls ceux connaissant la clé SK peuvent le déchiffrer. L'algorithme de chiffrement E et l'algorithme de déchiffrement D peuvent être différents mais il est possible de les rendre identiques.

Les algorithmes doivent être tels que

- les utilisateurs doivent être capables de calculer efficacement une paire de clés PK,SK
- la connaissance de PK ne doit pas rendre aisé le calcul de SK
- le déchiffrement d'un message chiffré doit redonner le message original, c'est-à-dire

$$D_{SK}(E_{PK}(X)) = X \text{ pour tout } X$$

Si on a aussi que $E_{PK}(D_{SK}(X)) = X$, l'algorithme peut servir à signer les messages.

On considère:

p, q deux nombres premiers secrets	
$r = p \cdot q$	connu
$\mu(r) = (p-1)(q-1)$	secret
clé SK	secrète
clé PK	connue
message X	secret
message chiffré Y	connu

Deux nombres a et b sont congruents modulo r si $a = b + cr$ avec c entier. On notera $a \equiv b \pmod{r}$.

Euler a démontré que

si a est premier avec r
 et si $\mu(r) = r \cdot (1-1/p_1) \dots (1-1/p_i) \dots (1-1/p_n)$, p_1, \dots, p_n étant les facteurs premiers de r .

alors $a^{\mu(r)} \equiv 1 \pmod{r}$

Remarque: $\mu(r)$ détermine combien de nombres sont premiers avec r .

Exemple: $\mu(20) = 20 (1-1/2) (1-1/5) = 8$ et les nombres premiers avec 20 sont 1, 3, 7, 9, 11, 13, 17 et 19.

Sachant que $a \equiv b \pmod{r} \implies a^m \equiv b^m \pmod{r}$ pour tout m , on a

$a^{\mu(r)} \equiv 1 \pmod{r} \implies a^{m\mu(r)} \equiv 1 \pmod{r}$

et

$a^{m\mu(r)+1} \equiv a \pmod{r} \quad (1)$

On choisit SK et PK tels que

$SK \cdot PK = m \mu(r) + 1$

c'est-à-dire

$SK \cdot PK \equiv 1 \pmod{\mu(r)}$

(1) devient alors $a^{SK \cdot PK} = a \pmod{r}$

Le chiffrement correspond à

$E_{PK}(X) = Y = X^{PK} \pmod{r}$

et le déchiffrement à

$$D_{SK}(Y) = Y^{SK} \pmod{r} = X^{PK.SK} \pmod{r} = X \pmod{r}$$

Grâce à la commutativité de la multiplication, les opérateurs peuvent être inversés:

$$D_{SK}(E_{PK}(X)) \equiv E_{PK}(D_{SK}(X)) \equiv X \pmod{r}$$

Pour que l'opération de chiffrement (ou de déchiffrement) soit une bijection, il faut que

$$0 \leq X \leq r-1$$

Rappelons que ces résultats ne sont valables que pour a (ou X) premier avec r . On peut cependant montrer que la relation

$$a^{m\mu(r)+1} \equiv a \pmod{r}$$

est valable pour tout a si $r = p.q$ avec p et q deux nombres premiers et $0 \leq a \leq r-1$.

En effet:

pour $a = 0$: la relation est triviale

pour a premier avec r : la relation est démontrée ci-dessus

pour a non premier avec r :

a contient soit p , soit q en facteur. Supposons que ce soit p : $a = cp$ avec c entier

$0 \leq a \leq r-1 \implies a$ est premier avec q (si ce n'était le cas, on aurait $a = c'pq \geq r$)

$$\text{On a alors } a^{\mu(q)} \equiv 1^{m(p-1)} \equiv 1 \pmod{q}$$

or $(p-1)\mu(q) = (p-1)(q-1) = \mu(r)$ de telle sorte que

$$a^{m\mu(q)} \equiv 1 \pmod{q}$$

Il existe donc un entier n tel que

$$1 = a^{m\mu(q)} + n.q$$

Multipliant les deux membres par $a = c.p$, on obtient

$$a = a^{m\mu(r)+1} + (n.q)(c.p) = a^{m\mu(r)+1} + n.c.r$$

$$\text{ou } a^{m\mu(r)+1} = a \pmod{r}$$

En résumé:

1. Deux nombres premiers p et q sont choisis aléatoirement
2. $r = p.q$ est rendu public
3. $\mu(r) = (p-1)(q-1)$ est calculé et gardé secret
4. SK premier avec $\mu(r)$ est choisi et gardé secret
5. PK inverse de SK modulo $\mu(r)$ est calculé et rendu public
6. Le chiffrement revient à élever le texte original découpé en séquence de caractères X tels que $0 \leq X \leq r-1$, à la puissance PK. Le résultat est le texte chiffré Y ($0 \leq Y \leq r-1$)
7. Le déchiffrement est effectué par l'élévation de Y à la puissance SK ce qui redonne X .

(3) Signatures digitales

L'authentification d'un message comprend:

- la vérification de l'identité de l'expéditeur
- la vérification de l'intégrité du message (celui-ci a-t-il été modifié lors de la transmission ?)

Si l'expéditeur et le destinataire ont confiance l'un dans l'autre, ces deux vérifications sont suffisantes. Il en est tout autrement s'ils se méfient l'un de l'autre:

- le destinataire peut composer un message et prétendre qu'il provient de l'expéditeur
- l'expéditeur peut envoyer un message puis en refuser la paternité

Une tierce personne ne peut faire la distinction entre ces deux cas. Seuls des algorithmes asymétriques permettent de résoudre ce problème.

L'emploi d'un système de chiffrement asymétrique avec une clé secrète permet au destinataire d'être certain de l'identité de l'expéditeur (puisque'il est le seul à posséder cette clé secrète). Mais dans ce cas, n'importe qui peut décoder le message. Si on désire qu'il ne soit pas lisible par tous, il faut coder le message une seconde fois avec la clé publique du destinataire rendant la connaissance de la clé secrète correspondante obligatoi-

re.

g. La cryptographie et les réseaux

Le chiffrement, dans un réseau de communications, peut se faire de deux façons:

- chiffrement de noeud en noeud: à chaque noeud du réseau, un message entrant est déchiffré, interprété et chiffré à nouveau avant de poursuivre son chemin. Cette procédure est nécessaire si les informations de routage se trouvent dans le message chiffré

- chiffrement d'extrémité à extrémité: l'émetteur chiffre le message qui transite par le réseau et est déchiffré par le destinataire. Les informations de routage doivent être transmises en clair mais les données n'apparaissent jamais en clair dans le réseau. Cette méthode permet l'utilisation de plusieurs clés par émetteur.

Dans le chiffrement de noeud en noeud, l'utilisateur n'a pas conscience de ce qu'un chiffrement est effectué (transparence). Le chiffrement d'extrémité à extrémité peut aussi être plus ou moins transparent si les opérations de chiffrement et de déchiffrement se font automatiquement.

Dans le cas d'une utilisation optionnelle du chiffrement, il faut veiller à l'indiquer dans le message par mise à 1 d'un bit particulier ou par envoi d'une séquence spéciale signifiant un basculement chiffré/non chiffré.

Etant donné que pour le chiffrement d'extrémité à extrémité, les informations de routage transitent en clair, une analyse malveillante du trafic, et donc du nombre de messages transitant d'un point à un autre, est possible.

Le chiffrement de noeud en noeud n'est intéressant que si le nombre de noeuds est petit. Les appareils de chiffrement aux noeuds opèrent en temps réel ce qui ne cause pas de retard dans la transmission. Ce chiffrement a aussi l'avantage que, vu sa transparence, il ne requiert aucune modification de logiciels existants. Les équipements de chiffrement doivent évidemment être compatibles (au niveau des protocoles de communication) avec les appareils auxquels ils sont reliés.

Si le chiffrement d'extrémité à extrémité est utilisé, les utilisateurs partagent une clé commune (ou une paire de clés dans le cas d'un chiffrement asymétrique). Cette clé est soit connue des opérateurs, soit stockée ou générée par l'appareil en cas de chiffrement transparent. Souvent une clé n'est utilisée que pour une seule communication: on l'appelle alors clé de session. Cette clé de session est générée par la sta-

tion maîtresse et est transmise à la station secondaire chiffrée par une clé connue des deux stations (clé chiffiante). Cette approche permet à chaque paire émetteur-récepteur de travailler avec une clé chiffiante propre. La découverte d'une clé chiffiante n'entraîne pas l'insécurité du système total.

Le secret des clés des récepteurs est sauvegardé en les stockant dans une zone protégée particulière appelée boîtier cryptographique sécurisé. L'accès en est réglementé et il ne doit pas être possible d'obtenir la clé en clair en dehors du boîtier sécurisé. Il est important que l'algorithme de chiffrement (le DES par exemple) se trouve également dans un boîtier sécurisé car la connaissance de valeurs intermédiaires de calcul peut mener à la découverte de la clé. Le boîtier doit permettre l'introduction des données à chiffrer et la sortie des résultats.

Les mêmes clés sont dans l'émetteur chiffrées par une clé maîtresse elle-même protégée par un boîtier sécurisé.

Les clés doivent être changées périodiquement et les règles de création de clés doivent être clairement déterminées.

Le boîtier sécurisé peut être un objet physique protégé par des dispositifs spéciaux (la carte à microprocesseur en est un exemple) mais aussi une routine logicielle. Dans ce dernier cas, la sécurité est assurée par la logique du programme mais la capacité de protection dépendra alors des fonctions du microprocesseur et plus particulièrement de la puissance de ses fonctions privilégiées: protection en écriture et lecture, modes d'exécution des programmes,... La sécurité apportée par cette solution logicielle n'est pas meilleure que celle du système d'exploitation.

7. La carte à mémoire

L'utilisation des cartes à mémoire est au goût du jour car:

- le support carte nous devient de plus en plus familier: badges d'identification, cartes de crédit, carte de club, de membre privilégié
- le contexte technologique est des plus favorables: progrès de la micro-électronique, intégration de plus en plus poussée des composants électroniques,...
- le besoin de sécurité grandit: il faut faire face aux nouvelles menaces engendrées par l'introduction des réseaux de télécommunication et par l'accroissement de la complexité des systèmes informatiques.

Le terme carte à mémoire est générique et englobe en fait plusieurs cartes différentes:

- les cartes à mémoire simple qui comme leur nom l'indique ne contiennent que de la mémoire (256 bits à quelques milliers de bits)
- les cartes à logiques câblées pouvant contrôler et gérer les accès à la mémoire (cartes MZ4, MZ9 et MZ 4608 de Schlumberger-Industrie et Siemens 4401). Le lecteur intéressé par la technologie de ces cartes peut consulter [GUE].
- les cartes à microprocesseurs qui font cohabiter dans une même puce de la mémoire et un microprocesseur permettant d'établir des dialogues complexes et un très haut niveau de sécurité (cartes Bull CP8, Philips M4, DES-D1 et DES-D2 et Thomson COS TS 1300 et TS 1301)
- les super smart card. Encore à l'état de prototypes, ce sont de véritables petits ordinateurs avec écran LCD, clavier, mémoire de 64 Kbits, processeur et alimentation par pile.

a. Le concept de carte à microprocesseur

Extérieurement, ce produit se présente comme une carte de crédit portant généralement le logo de l'émetteur et dont les dimensions satisfont aux normes internationales. Dans ce support de plastique (PolyVinyl de Carbonate ou autre), on perce un trou destiné à recevoir une pastille constituée d'un circuit imprimé qui contient un connecteur externe chargé de gérer le dialogue avec un lecteur et un composant placé derrière le circuit imprimé. Le connecteur externe appelé vignette est constitué de 8 contacts utilisés pour l'alimentation, la programmation (tension de programmation de l'EPROM), la masse, la remise à zéro, le signal d'horloge et une ligne série pour les entrées/sorties.

Les cartes actuelles sont mono-chip, c'est-à-dire qu'elles ne contiennent qu'un seul composant (circuit intégré) renfermant le microprocesseur, à savoir l'unité arithmétique et logique (ALU), l'unité de commande, les registres et accumulateurs de base, la mémoire, le bus et les circuits de sérialisation pour les échanges de données. Ce circuit intégré unique est souvent appelé Microcalculateur Autoprogrammable Monolithique (MAM).

Les protocoles d'échange entre la carte et le monde extérieur sont spécifiés dans la norme ISO 7816.

(1) La mémoire

Contrairement aux autres types de cartes (optique, magnétique,...) qui peuvent aussi mémoriser de l'information, la carte à microprocesseur possède plusieurs types de mémoires. Ainsi est-il possible de faire cohabiter sur le même composant des mémoires RAM (Random Access Memory), ROM (Read Only Memory) et EPROM (Electrically Programmable Read Only Memory) ceci sur une surface de quelques millimètres carrés (15 à 30 selon les composants). Dans la RAM (32 à 160 bytes) on trouve la mémoire de travail du micro-calculateur, tandis que dans la ROM (1.6 à 6 Kbytes), gravés de façon indélébile lors de la fabrication du composant, se trouve le logiciel de base: système d'exploitation et opérations élémentaires exécutées à la demande du calculateur. L'EPROM (1 à 8 Kbytes) reçoit quant à elle des informations indélébiles traduisant un certain nombre d'événements qui surviennent au cours de la vie de la carte ou contenant les données relatives au propriétaire ou à l'application.

La mémoire EPROM peut être complétée ou remplacée par une mémoire EEPROM (Electrically Erasable Programmable Read Only Memory) qui est une mémoire programmable effaçable supportant des données propres à l'application. Dans ce cas, l'efficacité de la sécurité est plus aléatoire car la mémoire peut être effacée à loisir. En outre, les cartes qui admettent ce type de mémoire sont souvent bi-composant (le second composant supporté par le circuit imprimé étant le calculateur lui-même), la fiabilité de l'ensemble et l'encombrement s'en ressentent.

(2) L'intelligence

L'ensemble des mémoires est complété par une unité de calcul (en général un microprocesseur 8 bits de type Motorola 6805, Intel 8048 ou TS1834 de Thomson) qui permet d'effectuer des opérations, d'exécuter un certain nombre de programmes contenus dans la carte. C'est l'intelligence proprement dite de la carte. Les logiciels gèrent les mémoires, exécutent des algorithmes, ... Chaque type de carte correspond à un programme particulier appelé masque. Un même masque offre la possibilité de gérer plusieurs applications dépendantes de la personnalité de l'EPROM.

Un modèle de cartes est caractérisé par:

- la division de l'EPROM en zones distinctes dont le chargement est réalisé par le fabricant, l'émetteur ou l'utilisateur

- les opérations disponibles: lecture, écriture, contrôle d'accès, validation, ...

(3) La modularité

On utilise ici les mémoires EPROM (et EEPROM le cas échéant). Elles reçoivent et conservent les données propres à chaque application. Certaines données sont écrites à la fabrication de la carte, d'autres au cours de la vie de la carte. Ces opérations se font sous contrôle de l'unité de calcul, ce qui interdit d'écrire directement dans la mémoire considérée. Le principal avantage de ce système est de pouvoir définir dans la mémoire de la carte des zones dont l'utilisation est particulière à l'application. On imagine aisément qu'en matière de contrôle d'accès la possibilité de gérer des droits et autorisations directement sur la carte de l'utilisateur offre une grande souplesse, d'autant plus que la mise à jour des droits des titulaires peut se faire aisément et quasiment en temps réel.

(4) La personnalisation

La personnalisation revient à donner un caractère unique à un objet fabriqué en série. Cette personnalisation peut se faire d'une part physiquement par impression de caractères en relief et/ou de logos représentant les émetteurs, d'autre part logiquement par écriture d'une information identifiante dans une zone de la mémoire.

(5) Les lecteurs de carte à mémoire

Le lecteur-encodeur sert à:

- initialiser la carte
- lire et écrire les données dans la carte (mémoires PROM et EPROM)
- chiffrer et déchiffrer (lorsque la carte ne peut le faire)

Le lecteur-encodeur est l'interface privilégié entre la carte et le monde extérieur. Il est pourvu d'une fente et d'un mécanisme de guidage de la carte. Un contacteur relie le lecteur à la carte, lui fournit son alimentation et transmet les données. Ce contacteur est lui-même relié à un microprocesseur accompagné de ses mémoires RAM, ROM, PROM et EPROM. Les fonctions réalisables par le lecteur dépendent de son utilisation et donc de son environnement.

Lorsque le lecteur est connecté soit directement à un micro-ordinateur, soit via un modem à une liaison téléphonique, la liaison est asynchrone V24/V28 (prise standard à 25 broches) et les vitesses de transmission vont de 1200 à 9600 bauds half-duplex. L'alimentation du lecteur peut se faire sur secteur, sur piles ou sur batteries. La réalisation d'un lecteur-encodeur propre à l'application est possible à partir d'éléments de base.

Les principaux lecteurs-encodeurs connectables à un micro-ordinateurs sont:

- les Bull TLP 124 et TLP 224
- les Schlumberger Industrie SCR 110 et SCR 150
- les Logicam LP-CAM/I, LP-CAM/A et LP-CAM/C
- le TRT-TI PE 111

Le lecteur-encodeur doit être pourvu d'un organe d'entrée du code identificateur de l'utilisateur et d'un écran permettant l'affichage d'ordres simples tels: "Introduisez la carte", "Composez votre code confidentiel", ... Si ce n'est pas le cas, c'est le micro-ordinateur raccordé qui devra assurer ces fonctions, les codes confidentiels transitant alors en clair sur la liaison.

On distingue les lecteurs intelligents, contenant le logiciel d'application et pouvant fonctionner seuls, des lecteurs transparents à l'application qui doivent recevoir les paramètres de l'application à chaque mise sous tension. Ces lecteurs ne contiennent pas d'intelligence propre dans le sens où ils sont conçus pour dialoguer avec le microprocesseur de la carte grâce à un ordinateur hôte, ce dernier ayant une couche logicielle applicative pour traiter les cartes.

Il existe des logiciels de simulation du comportement du lecteur-encodeur et de la carte qui sont exécutables par un micro-ordinateur ce qui offre une grande souplesse pour le développement: exécution pas à pas, visualisation de l'état du processeur, des zones mémoire, ... Cet émulateur permet également à l'utilisateur de se familiariser avec l'application.

Lorsque le nombre d'utilisateurs est limité, un des lecteurs-encodeurs peut servir à la personnalisation des cartes (moyennant bien sûr la connaissance d'une clé particulière) c'est-à-dire à l'écriture dans les zones carte et les lectures de contrôle, au choix et à l'affectation

d'un deuxième code porteur, au déblocage de cartes utilisées abusivement (3 essais erronés), à l'invalidation définitive des cartes.

(6) Les sécurités physique et logique

C'est essentiellement l'emploi de circuits intégrés et plus précisément leur petite taille qui assure l'intégrité physique des cartes. L'altération d'un de ses éléments requiert un matériel très coûteux, souvent hors de proportion avec le gain escompté par l'attaquant. Les organes de calcul et les mémoires peuvent aussi être protégés de toute intrusion physique par des dispositifs spéciaux tels des treillis parcourus par un courant continu détectant toute discontinuité en leur sein.

Le programme d'exploitation (masque) est aussi de nature à améliorer la sécurité. La confidentialité des données en carte est garantie par le fait qu'elles ne sont accessibles que si la clé est connue. La présentation d'une mauvaise clé entraîne un blocage de la carte. Le masque joue un rôle de censeur qui autorise ou refuse la sortie d'une partie du contenu de la mémoire. L'intégrité des données est aussi assurée, l'écriture étant impossible ou contrôlable à posteriori par la connaissance de la clé ayant servi à cette écriture.

Plusieurs ordinateurs dialoguant entre eux constituent un réseau. Ils peuvent être reliés par des lignes téléphoniques banalisées ou des lignes louées. Un tel système implique le transport d'informations sur les lignes de communication. Si ces informations sont confidentielles, elles doivent être protégées, les techniques de chiffrement étant alors les plus efficaces.

b. Les avantages de la carte à microprocesseur

La carte à microprocesseur est donc un objet facilement portable contenant une mémoire, de l'intelligence, modulaire dans ses fonctions, et offrant une sécurité physique et logique de très bon niveau.

Les avantages de la carte sont nombreux:

- la grande taille de la mémoire permet un important stockage d'informations. L'arrivée de cartes de 64 Kbits est imminente, ce qui apportera une grande souplesse dans certaines applications (dossiers portables)
- la capacité de calcul permet l'exécution d'algorithmes
- l'autoprotection permet de garantir l'identité du porteur,

l'authenticité des informations contenues et l'impossibilité de les altérer frauduleusement. L'utilisateur est en partie libéré de l'appréhension qui lui cause la perte ou le vol

- l'indébilite de la mémoire
- la possibilité d'utiliser la carte pour plusieurs applications (carte multiservice)
- l'impossibilité de reproduction
- la possibilité de connexion automatique grâce aux paramètres écrits dans la carte (augmentation de la convivialité)
- la taille réduite de la carte permet à l'utilisateur de l'emporter avec lui et d'en rester propriétaire
- les lecteurs gérant les cartes peuvent être simples d'emploi

La carte à puce, par la sécurité qu'elle permet d'apporter aux transactions par son caractère non reproductible et infalsifiable, apparaît comme l'un des moyens permettant de réduire considérablement les fraudes dues aux contrefaçons, aux cartes perdues ou volées, et aux manipulations frauduleuses de données.

En effet, l'un des atouts majeurs de cette carte tient à la présence du microprocesseur capable de vérifier lui-même que le code porteur qui lui est présenté correspond bien à la référence placée dans une zone secrète de la mémoire de la puce, lors de sa fabrication. De plus, elle possède une barrière infranchissable pour d'éventuels fraudeurs: elle se bloque au bout de trois fausses présentations de code. Seul l'émetteur peut alors la réhabiliter.

Le contrôle de la validité de la carte, qui sera effectué par la puce, garantit l'authenticité de celle-ci. En produisant un certificat de la transaction inscrit en mémoire de données elle apporte une preuve de la transaction effectuée qui pourra servir en cas de litige.

L'utilisation de la carte rend obligatoire la connaissance de la clé de chiffrement, ce qui s'avère très difficile pour le candidat fraudeur, étant donné que chaque carte possède une clé diversifiée qui est susceptible d'être changée du jour au lendemain.

c. Le cycle de vie d'une carte

La sécurité est assurée par le fait que chaque phase du cycle de vie d'une carte nécessite l'utilisation de droits d'accès donnés par la phase précédente.

(1) Phase de fabrication

La puce de silicium, contenant en ROM le système d'exploitation de mémoire de la carte, est raccordée à un circuit imprimé qui est ensuite fixé au support plastifié. Des données internes sont écrites dans la zone de fabrication (code fabricant, numéro de série) qui est ensuite verrouillée. Pendant cette phase, la carte est protégée par un code secret temporaire qui rend inopérant tout vol de cartes vierges.

(2) Phase de personnalisation

La carte est gravée (logo, photographie,...), des données non confidentielles (identification du porteur) et des données secrètes (code émetteur, code porteur, clés secrètes) sont inscrites en zone mémoire. On inscrit également en mémoire des données qui définissent l'utilisation, la taille et le mode d'accès des différentes zones de la mémoire. Le code secret de fabrication est mis hors service et la zone de personnalisation est verrouillée et rendue secrète.

(3) Phase de distribution au porteur

(4) Phase d'utilisation

Il s'agit ici de l'utilisation de la carte par le porteur ou par l'émetteur. Seule la zone de transaction peut être accessible. C'est le masque qui définit sa structure qui pour la carte BULL CP8 est la suivante:

- zone secrète accessible par le microprocesseur uniquement
- zone de transaction protégée par un code (émetteur ou porteur)
- zone de lecture libre pour les informations non confidentielles
- zone de contrôle d'accès mémorisant les accès aux zones de transactions protégées.

(5) Phase de fin de vie

La carte est bloquée en cas de remplissage de la zone mémoire gérant les accès ou en cas d'invalidation par le monde extérieur.

Données inscrites au cours de la phase		Conditions d'accès en lecture
fabrication	code fabricant numéro de série	libre
personnalisation	identification du porteur	libre
personnalisation	codes confidentiels, clés secrètes	zone secrète
utilisation	transactions	code émetteur ou code porteur

d. Fonctionnement de la carte BULL CP8

(1) Caractéristiques techniques

Le circuit intégré renferme un microprocesseur 8 bits (Motorola 6805 ou Intel 8048), une ROM, une RAM et une PROM.

Il existe plusieurs modèles de cartes, chacune avec leurs tailles mémoires particulières:

	Techno- logie	Unité centrale	Fabricant du circuit
CP8 01	HMOS	6805 (8 bits)	Motorola
CP8 02	HMOS	8048 (8 bits)	Euro- technique
CP8 03	HMOS	6805 (8 bits)	Motorola
CP8 11+12	CMOS	(8 bits)	
CP8 21	CMOS	(8 bits)	
TS 1821		(8 bits)	
TS 1834		(8 bits)	
M4		(8 bits)	
D1		(8 bits)	

	Taille mémoire (en octets)				Algorithme de chiffre- ment
	RAM	ROM	EPROM	EEPROM	
CP8 01	36	1.6K	1K	-	Télépass
CP8 02	44	2K	1K	-	Télépass
CP8 03	52	2K	2K	-	Télépass
CP8 11+12	128	4K	8K	-	Télépass
CP8 21	128	4K	-	2K	Télépass
TS 1821	44	2K	1K	-	
TS 1834	76	3K	4K	-	
M4	36	1.6K	1K	-	Télépass
D1	44	2K	1K	-	DES

La ROM contient un masque qui s'occupe de:

- la gestion physique et logique des échanges d'informations entre la carte et le monde extérieur (lecteur)
- la gestion de l'accès à la mémoire EPROM
- le calcul de la fonction TELEPASS non réversible

Le développement d'un masque spécifique est très coûteux, de l'ordre de plusieurs millions de FB. Il est donc impensable de concevoir un nouveau masque si l'application ne met en jeu qu'un petit nombre de cartes.

Le masque standard actuel de la carte CP8 est le M4 version B0. Les fonctionnalités sont activées de l'extérieur grâce à un jeu d'ordres élémentaires. Il permet de travailler sur la mémoire utile (EPROM) segmentée en zones: zones sécuritaires, zones de données et zone de fabrication. L'accès à ces zones est réglementé en fonction des degrés de confidentialité des informations contenues. M4 contient l'algorithme Télépass.

Le masque MP (Multi-Purpose) est développé dans la perspective d'une carte multiservice: il permettra de faire cohabiter sur la même carte plusieurs applications totalement indépendantes.

Le masque M4 est disponible sur les EPROM 1K, le MP sur les EPROM 8K et les EEPROM 2K. L'EPROM 2K contient le masque M9 très semblable au M4.

(2) Enchaînement des opérations

- Il y a d'abord comparaison des codes secrets présentés par l'utilisateur et des codes inscrits en zone secrète de la mémoire. Si la comparaison est satisfaisante, la suite des opérations est autorisée
- Un calcul algorithmique authentifie les données mémorisées dans la carte et génère des clés de chiffrement/déchiffrement (sans transport de ces clés)
- L'utilisation de la mémoire par le monde extérieur est contrôlé (contrôle paramétrable lors de la personnalisation de la carte)

Le microprocesseur exécute les ordres issus du lecteur (lecture, écriture,...) et est capable de stocker et d'exécuter des algorithmes de chiffrement. La PROM est réservée à l'utilisateur et son accès est contrôlé par le microprocesseur. La RAM est inaccessible de l'extérieur et sert de mémoire de travail.

La carte permet la lecture et l'écriture mais aussi la certification et le chiffrement des données utilisateurs grâce à ses fonctions de calcul.

(3) Les fonctions de base

La structure générale d'un ordre carte est codée sur 5 octets (norme ISO).

NOM	INS	A1	A2	L
-----	-----	----	----	---

NOM étant le nom de l'application

INS le code instruction

A1 et A2 l'adresse en mémoire

L la longueur en octets

L'exécution d'une des instructions renvoie deux octets de statut ME1 et ME2. Les différentes erreurs possibles sont:

pour ME1

- longueur incorrecte de l'ordre
- adresse incorrecte
- ordre inconnu
- application inconnue

pour ME2

- zone d'état pleine
- carte bloquée
- carte muette
- clé émetteur fausse
- clé porteur fausse

Un ordre d'initialisation démarre le dialogue avec la carte et en donne les caractéristiques physiques: protocole de transfert, fréquence d'horloge, tension et intensité de courant de programmation, numéro de masque, numéro de fabricant, taille mémoire, état interne de la carte, etc...

(a) Ordres de présentation de clé

i) Présentation clé émetteur ou porteur

Ces ordres permettent de contrôler l'accès aux informations écrites dans la zone de transaction.

INS = 10: présentation de la clé émetteur 1A

INS = 20: présentation de la clé porteur 2A/2B ou de la clé de fabrication

INS = 30: présentation de la clé émetteur 1B

Le tampon contenant l'ordre est complété par la clé émetteur ou porteur.

Si la clé est correcte, les différentes protections de la zone de transaction définies lors de la personnalisation de la carte sont déverrouillées. Si la clé est fausse, l'accès aux informations n'est plus autorisé. La carte est bloquée après une présentation d'une fausse clé émetteur ou trois présentations d'une fausse clé porteur.

ii) Réhabilitation

L'ordre de réhabilitation permet de rendre valide la carte qui a été bloquée. Il nécessite la présentation simultanée de la clé émetteur et de la clé porteur.

(b) Ordres de lecture

i) Validation d'accès en lecture

Lors de la présentation de la clé porteur, la carte ne signale jamais si le code est correct, seul l'ordre de validation permet la détection de la présentation une ou plusieurs fois d'un faux code.

ii) Lecture d'octets

Cet ordre permet la lecture d'un certain nombre d'octets (nombre spécifié dans l'ordre). Si la carte est en lecture protégée, l'accès ne sera possible que si la clé porteur ou émetteur a été présentée au préalable suivi d'un ordre de validation en lecture. La carte reste muette si les conditions ne sont pas respectées.

(c) Ordres d'écriture

i) Ecriture d'un mot

Cet ordre permet d'écrire un mot de 32 bits sur la carte. Le premier bit sert au verrouillage (voir point suivant), les deuxième et troisième bit permettent de retrouver la clé ayant permis l'écriture.

ii) Validation d'écriture d'un mot

Cet ordre permet de verrouiller un mot en carte en faisant basculer le premier bit du mot à 0. Toute réécriture du mot est alors impossible. La clé ayant servi à l'écriture est obligatoire pour la validation.

(d) Fonction Télépass

i) Exécution d'un calcul

Un algorithme de calcul, Télépass, est intégré à la carte. Il s'agit d'une fonction à deux variables (le tampon contient ces deux variables).

ii) Demande de résultats

Le résultat de l'exécution de la fonction Télépass n'est accessible que par cet ordre.

(e) Ordre d'écriture des verrous

Cet ordre permet de positionner à 0 le ou les verrous situés dans la zone des verrous.

(4) Organisation de la mémoire

La mémoire EPROM est divisée en 7 zones de taille, de contenu et de mode d'accès spécifiques. Certaines zones sont personnalisées en lecture libre ou protégée et/ou en écriture libre ou protégée. Seule la zone confidentielle est facultative. L'adresse de début et de fin de carte sont fixes, les autres variables.

0200h	1 zone secrète
ADM	2 zone d'accès
ADC	3 zone confidentielle
ADT	4 zone transaction
ADL	5 zone lecture
ADF	6 zone fabrication
09F8h	7 zone des verrous

tableau 4: Carte à microprocesseur: organisation de la mémoire

La zone secrète contient les clés émetteur primaire 1A et secondaire 1B (il peut donc y avoir deux émetteurs) et la clé porteur 2A ou 2B. La clé 2A correspond au code confidentiel classique des cartes de crédit et peut être remplacée par son équivalent 2B sur demande du porteur. Les clés 1A, 1B et 2A sont inscrites en phase de personnalisation sous contrôle de la clé de fabrication.

La zone d'accès permet la mémorisation des résultats des présentations d'une des trois clés de la zone secrète.

La zone confidentielle est écrite durant la phase de personnalisation. Elle ne peut être accédée qu'en lecture sous présentation d'une clé.

La zone de transaction contient toutes les informations liées à l'application. L'accès en lecture ou en écriture au contenu de la zone de transaction peut nécessiter

la présentation d'une clé si l'on déclare cette zone en lecture ou en écriture protégée.

La zone lecture est libre d'accès et est remplie lors de la phase de personnalisation.

La zone de fabrication est écrite lors des phases de fabrication et de personnalisation. Elle contient les pointeurs des différentes zones, le type d'application, le numéro d'encarteur et le numéro de série, le type de protection d'accès associé à la zone de transaction.

La zone des verrous contient des verrous permettant de déterminer la phase de vie de la carte et le code porteur utilisé (2A ou 2B). Un des verrous permet d'invalidiser définitivement la carte.

Zones	Lecture	Ecriture
secrète	accessible en interne par le μP	interdite sauf création clé 2B
accès	sous contrôle des clés	accessible par le μP
confidentielle	sous contrôle des clés	interdite
transaction	libre ou sous contrôle des clés	libre ou interdite par verrouillage
lecture	libre	interdite
fabrication	libre	interdite
verrous	libre	écriture du verrou 2B ou du verrou d'invalidité

tableau 5: Zones de la carte à microprocesseur

Les cartes Philips DES-D1 sont très semblables aux CP8. Elles s'en différencient cependant par l'algorithme de chiffrement utilisé: il s'agit ici du DES (III.C.6.c).

Les cartes COS (Chip Operating System) de Thomson sont caractérisées par une gestion dynamique de la mémoire et

par la possibilité qu'a l'utilisateur de créer du code exécutable stocké en carte ce qui permet de définir une organisation mémoire propre et éventuellement l'extension des fonctions de base.

e. La sécurité logique

(1) L'identification du porteur de la carte

On considère un serveur central A et un utilisateur B éloigné de ce serveur. L'utilisateur possède une carte à microprocesseur dotée d'une fonction de calcul f et d'un secret S_b partagé avec le serveur (celui-ci est donc capable de reconnaître les cartes qui lui sont rattachées). La carte sera introduite dans un lecteur relié à un terminal lui-même relié au serveur.

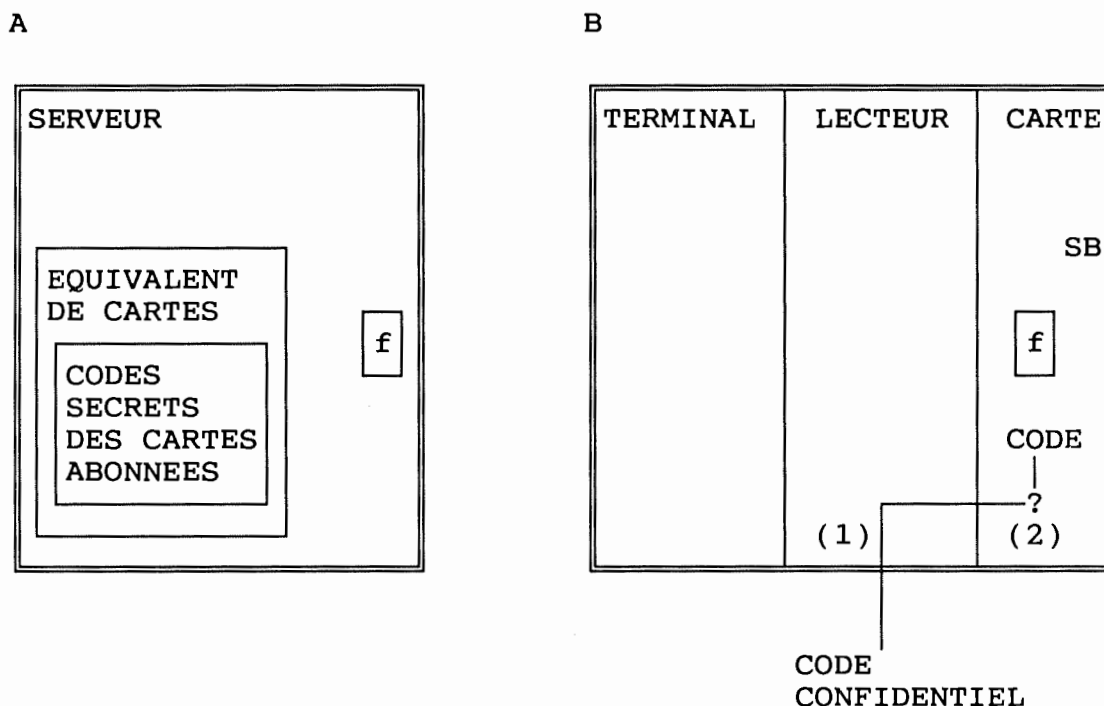


fig 11: Identification du porteur de la carte

L'utilisateur B introduit sa carte dans le lecteur connecté (ou intégré) à un appareil (terminal Minitel, micro,...). Il frappe son code confidentiel (de préférence sur un clavier intégré au lecteur) (1). La carte identifie alors le porteur (avec toutes les limites imputables à l'utilisation des codes confidentiels) (2). L'identi-

fication du porteur se fait donc au sein de la carte à puce et non par le terminal comme c'est le cas pour les cartes magnétiques.

(2) L'authentification

Il s'agit ici de l'authentification du récepteur par l'émetteur, la procédure symétrique permettant une reconnaissance réciproque.

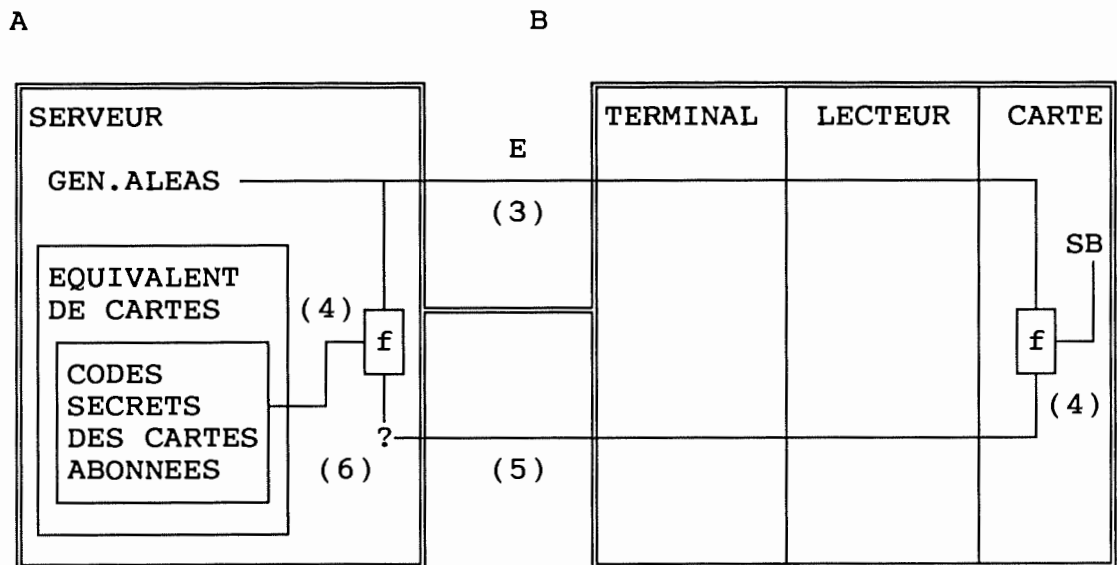


fig 12: Authentification du porteur de la carte

Une fois l'identité du porteur établie, la carte de B va converser avec son équivalent placé en A ⁽¹⁾. A fournit à B un aléa E (3) et chacun effectue un calcul de son côté (4).

Pour B: $R_B = f(E, S_B)$

Pour A: $R_A = f(E, S_A)$

f étant par exemple la fonction exécutée par l'algorithme DES.

B envoie son résultat à A (5), A compare R_B et R_A (6), si ceux-ci s'accordent l'authentification est déclarée

⁽¹⁾ Cet équivalent est en fait une super carte à microprocesseur encore appelée processeur de sécurité. Plus de détails à ce propos peuvent être trouvés dans [HUB]

bonne. Les deux entités peuvent s'échanger des informations.

Une procédure assez semblable à l'authentification est la certification. Elle consiste à s'assurer qu'une information bien précise se trouve en un certain endroit dans la carte: c'est alors le contenu de la cellule mémoire testée qui est utilisée en lieu et place du secret S_p .

(3) L'authentification par le récepteur

L'authentification du serveur par le récepteur peut se faire de la même manière mais il faudrait alors que la carte connaisse le code secret de l'émetteur ce qui d'un point de vue sécuritaire n'est pas souhaitable. On préférera alors l'emploi d'un algorithme de chiffrement à clé publique: l'émetteur A envoie un message codé avec sa clé secrète et B s'il parvient à le décoder grâce à la clé publique de A est certain de son origine. Le contenu de ce message codé est par exemple un condensé d'un message préalablement transmis.

(4) La confidentialité par le chiffrement

De par son intelligence, une carte à puce est capable d'exécuter un algorithme de chiffrement rendant possible le codage d'un texte en son sein. L'avantage de cette formule est que la clé de chiffrement ne quitte pas la carte et ne doit même pas être connue de l'utilisateur.

Le rôle du codage est de rendre un message confidentiel inintelligible à tout autre que le destinataire légitime (confidentialité) en permettant à celui-ci de reconnaître l'émetteur du message (authentification) et d'être assuré que ce message n'a pas été mal intentionnellement modifié ou créé (intégrité).

(5) La répudiation illicite

L'emploi d'un algorithme de chiffrement non symétrique (à clé publique) permet de résoudre ce problème:

- il faut empêcher qu'un autre que l'émetteur (y compris le récepteur lui-même) n'envoie le message en prétendant être l'émetteur: le message est codé avec la clé secrète de l'émetteur

- il faut que l'émetteur puisse prouver qu'il l'a bien envoyé au récepteur: celui-ci renvoie un accusé de réception codé avec sa clé secrète.

(6) La gestion des droits

On suppose un ensemble d'utilisateurs {a,b,c} et un ensemble de fichiers F {f₁, f₂, f₃, f₄} avec comme possibilité les droits suivants L: lire, C: créer, M: modifier.

Un exemple de matrice des autorisations serait:

	a	b	c
f ₁	L	LC	LM
f ₂	LCM	LC	LM
f ₃	LC	C	L
f ₄	LM	L	LM

On peut fabriquer 3 cartes A,B,C avec dans chacune d'elles les éléments suivants figurant en mémoire:

Fichiers [f₁], [f₂], [f₃], [f₄]

Cartes	[A]	[B]	[C]
lire	[0.0.0.0]	[0.0.1.0]	[0.0.0.0]
créer	[1.0.0.1]	[0.0.0.1]	[1.1.1.1]
modifier	[1.0.1.0]	[1.1.1.1]	[0.0.1.0]

avec pour convention 0: droit ouvert, 1: droit fermé.

Un bloc décrit le droit: un mot décrit les fichiers, un autre applique la matrice.

Bloc créer

Mot 1: f₁, f₂, f₃, f₄

Mot 2: 0, 1, 1, 0

Ainsi, on peut aisément s'apercevoir qu'il est possible de changer les droits carte par carte et fichier par fichier. Afin de se prémunir contre un changement intempestif, il est possible de signer (c'est-à-dire de s'assurer de l'intégrité des données initialement stockées) chaque enregistrement correspondant à un droit.

f. Les applications des cartes à mémoire

Les cartes à mémoire simple servent généralement de cartes de validation ou de prépaiement. Elles ont l'avantage d'être bon marché.

Les cartes à logiques câblées, dont les capacités mémoire sont comparables aux cartes à microprocesseur permettent la mise en place de système de sécurité de niveau satisfaisant. La logique étant câblée, les caractéristiques de la carte et donc les procédures sont figées.

Les cartes à microprocesseur permettent les applications à haut niveau de sécurité, les algorithmes de contrôle faisant partie du circuit. Cependant leur prix de revient est assez élevé et ce d'autant plus que le nombre de cartes commandées est petit.

On distingue trois classes d'applications:

- les applications faisant appel à des cartes de paiement, normalisées et émises par les banques

- les applications utilisant les cartes comme dossiers portatifs dont la carte santé, contenant les indications sur certains faits médicaux se rapportant en particulier aux traitements d'urgence, est un exemple. La lecture et l'écriture des informations y est possible. Les dossiers portatifs permettent aux usagers de rester propriétaires d'informations les concernant. Les informations ne sont accessibles qu'aux personnes habilitées qui peuvent les modifier ou les consulter.

- les applications où la carte sert de moyen d'accès: ouverture de portes, accès à un logiciel protégé contre la copie, à un serveur central, consultation à distance de bases de données,... Les applications faisant appel aux réseaux (transferts d'informations interbancaires, messagerie,...) exigent une authentification réciproque. Dans ces applications, les cartes servent à authentifier les partenaires mais aussi à chiffrer les messages échangés pour garantir leur confidentialité.

Dans un futur proche, les cartes disposant de mémoires plus vastes, elles pourront être multi-applications, des zones précises correspondant à chacune de ces applications.

Le choix de la carte est subordonné à la réponse à certaines questions:

- quel est l'usage majeur de la carte ? Est-elle mono ou multi-application ?

- quel est le niveau de sécurité exigé dans l'identification et l'authentification du porteur ?

- quel est le niveau de sécurité exigé dans l'autorisation d'exécution de telle ou telle fonction ?

- qui distribue les cartes et qui les gère ?

g. Problèmes liés à la carte à puce

(1) Capacités mémoire limitées

Les cartes à puce actuelles ne possèdent que de petites capacités de mémorisation. Ce n'est qu'après un accroissement substantiel que des applications stockant toutes leurs informations dans les cartes pourront être envisagées. Actuellement seules des applications de sécurité (identification, authentification, certification,...) sont réalisées.

(2) Lenteur des traitements

Les algorithmes de chiffrement sont très complexes et demandent donc un temps d'exécution assez grand ce qui influence négativement le débit maximum réalisable et interdit la manipulation de gros volumes de données en des temps acceptables.

(3) Rigidité de l'application

Le programme étant placé en mémoire morte, il est non modifiable et, le marché étant encore fort étroit, les applications disponibles sont générales, c'est-à-dire souvent mal adaptées à une application particulière. Les constructeurs sont à la recherche d'une solution à ce problème: la carte D2 de Philips permet par exemple un codage optionnel.

h. Evolutions

Les progrès technologiques permettront d'utiliser des microprocesseurs 16 et 32 bits et des mémoires de plus en plus grandes (doublement de la capacité tous les deux ans). Des algorithmes complexes pourront alors être intégrés et la carte pourra prendre en charge de plus nombreuses fonctions de sécurité, fonctions actuellement effectuées au sein du lecteur-encodeur, ce qui fragilise le système.

Une augmentation de la capacité mémoire permet une plus longue durée d'utilisation et l'emploi de mémoires réinscriptibles permettra d'étendre le champ des applications (effacement des données périmées,...).

8. Les autres cartes

a. La carte à piste magnétique

Le domaine des cartes permet à la technologie de donner le meilleur d'elle-même. A côté de la carte à microcircuit qui, en raison de ses fonctionnalités et de son haut niveau de

sécurité valait un paragraphe spécifique, on trouve d'autres types de cartes telles que la carte laser, la carte à lecture optique, et surtout la carte magnétique qui reste la plus connue et la plus utilisée. Elle est capable de stocker quelques octets d'information (les caractéristiques de l'utilisateur) et peut se protéger par un code confidentiel. Il faut noter que dans ce cas c'est un dispositif interne à l'appareil, dans lequel la carte est lue, qui possède l'algorithme de vérification du code confidentiel. Ses limites sont bien connues, surtout dans le monde bancaire puisque la fraude sur les cartes magnétiques est courante (duplication, création, falsification). Il existe néanmoins certains procédés qui permettent d'éviter la simple recopie de ce type de support et qui empêche, par la même occasion, toute falsification.

b. La carte d'identification

Elle se présente comme une petite calculette capable de générer un code confidentiel à partir d'une information émise par le serveur. Ce code est tapé au clavier du terminal par l'utilisateur et est vérifié par l'ordinateur distant. Ce système présente de multiples intérêts, on peut citer notamment: le changement de code confidentiel à chaque transaction ou session de l'opérateur, l'avantage d'avoir un support portable, le fait de s'affranchir de toute connexion physique avec le terminal...

Pourtant ce système reste fragile car le possesseur de la carte peut usurper l'identité de son propriétaire. On peut aussi considérer que la sécurité d'une telle solution repose essentiellement sur la solidité de l'algorithme de vérification et du générateur d'aléas installés sur le serveur ainsi que sur la fonction de calcul de la carte.

c. Le bouchon

C'est une véritable serrure pour des terminaux de type micro-ordinateurs. Le bouchon se connecte sur une sortie série (RS232C) du micro et autorise au seul détenteur l'exécution de certaines opérations. Ce produit est bien adapté à la protection des logiciels. Toutefois son utilisation paraît trop restrictive et sa sécurité d'un niveau trop sommaire pour protéger des logiciels ou des fichiers sensibles.



fig 13

IV. Critères d'évaluation

A. Relevé des critères

Sont repris ici les différents critères d'évaluation de systèmes de transmission tels qu'ils ont pu être dégagés des chapitres précédents. Il est à noter que, dans la plupart des cas, la satisfaction du critère n'a pas un caractère obligatoire: il s'agit souvent de souhaits que l'on désire voir exaucés. Ces critères doivent être pondérés suivant:

- leur importance intrinsèque
- la prise en compte d'autres critères (certains ne sont pas indépendants)
- le système considéré et plus particulièrement sa complexité (nombre de laboratoires et nombre de médecins impliqués, importance du trafic, ...)

Une pondération est reprise au point IV.C. Elle est destinée à l'évaluation d'un système de transmission de résultats d'analyses reliant un seul laboratoire à une dizaine de médecins et dont le trafic journalier est peu important (de l'ordre d'une vingtaine d'analyses).

Le cas échéant, certaines pondérations sont commentées au point IV.D.

1. Critères juridiques

Le Conseil National de l'Ordre des Médecins formule une éthique et promulgue les règles à respecter en matière d'échanges d'informations informatisées entre les laboratoires de biologie médicales, les médecins praticiens et les patients. Cet Ordre est donc un point de passage obligé pour la mise en place d'un système de transmission. (1)

La finalité de la collecte de données doit être connue des patients et vérifiée. Les données doivent être adaptées à cette finalité. La durée de conservation des données ne doit pas être excessive. (2,3,4,5)

Les données doivent être obtenues et traitées loyalement et licitement. Chacun doit pouvoir consulter et faire corriger les données le concernant (cette correction doit évidemment être justifiée). Les données doivent être exactes et mises à jour. (6,7,8)

Le malade doit être informé que le laboratoire et le médecin généraliste sont équipés d'un ordinateur et que moyennant son approbation le médecin demandeur de ces examens a accès à ses

résultats. Le malade a aussi la possibilité de donner le nom d'autres médecins qu'il désigne à cet effet. Le Dossier patient doit donc permettre la consultation par plusieurs médecins traitants (un médecin n'est toutefois pas obligé de communiquer ses notes personnelles). On doit pouvoir poser un verrou sur certains résultats empêchant leur transmission par voie téléinformatique. Dans ce cas les résultats ne pourront être communiqués que par compte-rendu imprimé étant bien entendu que le biologiste pourra toujours en cas de nécessité et dans l'intérêt du malade communiquer lui-même ses résultats par téléphone. (9,10, 11)

Le consentement écrit des personnes concernées pour le stockage et la transmission d'informations est nécessaire. (12,13)

Le respect de la vie privée et du secret médical doit être assuré par la confidentialité des données. (14)

2. Critères déontologiques

La standardisation au niveau du matériel permet une protection vis-à-vis de monopoles. (1)

La supervision par un médecin de l'Ordre des Médecins peut être requise. (2)

Pour être accessible, le dossier d'un malade devra obligatoirement avoir été validé par le médecin biologiste du laboratoire et cela de façon apparente dans le dossier du malade. (3)

Outre le respect du secret médical, il faut aussi garantir la liberté de choix du patient: choix du laboratoire et choix du mode de transmission des résultats. (4)

Un meilleur traitement de l'information (tenue à jour informatisée de dossiers médicaux, transmission de résultats par réseaux, ...) ne peut constituer un argument de choix par le patient d'un médecin préférentiellement à un autre. Autrement dit, on ne peut considérer l'informatisation comme un critère de qualité. Aucune publicité ne peut être faite pour la promotion du système de transmission. Le service ainsi rendu ne peut être payant. (5,6)

Le serveur doit être passif: seules les informations demandées peuvent être transmises à l'exclusion de toute autre ce qui implique la sélection obligatoire des données lues. (7)

La transmission des comptes rendus d'analyses ne peut se faire via un organisme intermédiaire distinct du laboratoire exécutant: le laboratoire exécutant est son propre serveur. La transmission directe des résultats du labo au patient est également à proscrire. (8,9)

La définition et les limitations des conditions de transfert (consultation ou envoi) d'un dossier doivent être clairement établies. (10)

Il ne doit pas y avoir de prise en charge des frais de télétransmission par le labo, des droits de location,... qui influencerait le médecin dans son choix. (11)

Les transmissions téléinformatiques ne peuvent se substituer aux autres moyens de transmission: une confirmation écrite est nécessaire. (12)

Il doit être possible d'interdire globalement la transmission de certaines classes de résultats. (13)

Le laboratoire ne peut avoir accès aux Dossiers médicaux du médecin prescripteur et le médecin ne peut avoir accès aux résultats qui ne concernent pas ses patients (cloisonnement des dossiers médicaux). (14)

3. Critères technologiques

Seul le cas de lignes téléphoniques RTT banalisées avec adaptation par modems sera retenu, essentiellement en raison des coûts prohibitifs des autres solutions (lignes louées à la RTT, ...).

Afin de garantir une opérationnalité maximum, il pourra être nécessaire d'exiger du fournisseur de matériel (ordinateurs, modems, lecteurs de cartes à microprocesseur,...) un dépannage endéans un certain délai (plus ce délai est court plus la dépense est importante). Cette possibilité de secours immédiat peut être rendue inutile par l'emploi de systèmes redondants. (1,2)

Les réactions suite à une panne des mécanismes de protection ou du matériel doivent être bien déterminées. Il faut par exemple lors d'une panne de la mémoire de masse garantir l'effacement des données stockées avant l'envoi en réparation. (3)

Il faut s'assurer de la fiabilité de la transmission des données grâce à la détection et la correction des erreurs de transmission. Les erreurs dues au traitement et au stockage doivent aussi être contrôlées. (4)

Les débits moyens et maximum doivent être supportables par le réseau. (5)

Le compactage des données permet de rentabiliser la transmission. (6)

Le système doit être ergonomique: simple et facile à mettre en oeuvre, connexion automatique, transmission, chiffrement et compactage transparents. (7,8,9,10,11)

Les investissements doivent se faire à coût minimum, la dépense par unité d'information transmise doit être petite. (12)

Des extensions au système doivent être possibles ce qui permettra un meilleur amortissement des investissements. (13)

Une standardisation du logiciel ou au minimum du format d'échange permet d'interconnecter des systèmes différents. (14,15)

La plupart des malfonctionnements de programmes peuvent être évités par l'emploi de logiciels de qualité (mais cher !). Le matériel doit lui aussi être choisi avec soin. (16,17)

Le système doit permettre une mise en évidence de résultats anormaux (au sens médical) ainsi qu'une mention de la possibilité d'inexactitude suite à des modifications légales ou accidentelles de l'identité du patient, la possibilité de verrouillage d'une partie des renseignements, le dépassement de capacité d'archivage. (18,19)

Comme pour tous les systèmes informatiques, il est nécessaire d'archiver les données et d'en faire des copies. L'accessibilité aux anciens résultats doit être garantie. L'archivage des messages peut aussi être utile. (20,21,22)

La limitation de la durée de consultation permet d'éviter le blocage de la ligne due à une déconnexion non effectuée. (23)

Il faut prévoir la possibilité de transmettre des messages personnels du médecin biologiste aux médecins et vice-versa et rendre obligatoire la consultation de certains messages importants. (24,25)

Dans le cas d'un serveur central au laboratoire contenant les données en consultation, l'installation de plusieurs lignes ou la réservation de plages horaires par médecin peut être requise si le trafic est important. (26,27)

L'impression de messages sur papier doit être possible. (28)

Les relevés statistiques (nombre d'appels, durée moyenne des appels, nombre de kB transmis, analyse du contenu) permettent d'évaluer le système. (29)

4. Critères sécuritaires

Une spécification correcte de la politique de sécurité par les autorités de gestion est nécessaire (voir IV.B) (1)

Les terminaux doivent être situés dans un environnement sécurisé: l'accès à la salle d'ordinateurs doit être filtré. (2)

L'initialisation sécurisée du système doit être requise: une seule procédure de lancement doit être possible et celle-ci ne peut être exécutée par une personne non autorisée. (3)

L'identification de l'opérateur doit être possible et obligatoire, soit grâce à un code confidentiel connu de lui seul, soit par une caractéristique qui lui est propre (possession d'une carte à microprocesseur, caractéristique biologique,...) ou une combinaison des deux. (4,5,6,7)

L'authentification, c'est-à-dire la reconnaissance à distance de l'identité du correspondant, peut se faire par la procédure décrite en III.C.7.e.(2). Elle requiert l'utilisation d'une carte à microprocesseur. L'échange de mots de passe est une seconde possibilité nettement moins sécurisante et à proscrire si aucun chiffrement n'est fait sur la ligne. (8,9)

La confidentialité et l'intégrité sur la ligne sont assurés la plupart du temps par le chiffrement des données transitant sur la liaison. Ce chiffrement peut être fait dans le terminal ou par une carte à microprocesseur. (10,11,12,13)

Il faut s'assurer que l'algorithme de chiffrement est performant et bien utilisé. (14,15)

L'autorisation d'accès au réseau doit être subordonné à une identification correcte. (16)

Il faut prévoir une conservation des traces de transfert des dossiers (journalisation) reprenant l'identité des partenaires, l'identité du dossier, les dates et heures de transfert et l'enregistrement de la dernière demande de connexion de chaque côté et sa comparaison lors de la demande suivante. (17,18)

L'inventarisation des matériels permet de déceler les vols et de prendre les mesures correctives. Cet inventaire et la non proximité de moyens de reproduction des documents (photocopieuses, ...) permet de se protéger contre les copies. (19,20)

La protection contre la fuite illégale d'informations autorisées ne peut se faire que par une sélection appropriée des personnes ayant accès au système. (21)

L'adéquation du comportement de l'application aux spécifica-

tions doit être vérifiée: la découverte de fonctions "inutiles" peut mener à la découverte de procédure de contournement ou de désactivation des mécanismes de sécurité par les programmeurs de systèmes et de l'installation de systèmes non sûrs. (22)

Des assurances contre les désastres naturels (incendies, inondations, ...) doivent être contractées. (23)

Dans le cas d'un serveur central contenant les données en consultation, le numéro d'appel du serveur peut être privé c'est-à-dire non communicable par la RTT. (24)

Le numéro d'appel peut aussi être secret, non connu de l'appelant. (25)

Les clés d'identification, d'authentification et de chiffrement doivent être aisément modifiables. (26)

Elles doivent être modifiables par l'autorité reconnue uniquement. (27)

Il faut assurer une identification certaine du malade notamment par l'emploi d'un numéro identifiant national ou d'un identifiant local. (28)

Un accès direct à l'ordinateur du laboratoire permet l'utilisation de la banque de données ce que ne permet pas un accès via une boîte aux lettres. C'est pourtant ce dernier moyen qui est préféré pour rendre impossible la consultation du reste des données. Il faut également veiller à prévenir les consultations accidentelles des autres informations du serveur. Les ordinateurs de transfert et ordinateur central peuvent être physiquement séparés. (29,30)

La gestion et la supervision d'un système de cartes sera réservé à des institutions contrôlées par l'Etat ou à des autorités publiques compétentes en matière de politique de soins de santé. Ce critère peut, au premier abord, paraître difficile à satisfaire. Tant que les systèmes sont de petites tailles et encore au stade expérimental, la constitution d'institutions indépendantes des médecins et des patients n'est pas nécessaire. Elle le deviendra lorsque, les systèmes s'étendant à un grand nombre de laboratoires et de médecins, certaines règles devront obligatoirement être respectées par tous. (31,32)

Les transmissions des résultats par téléphone ou par courrier ne sont pas d'une fiabilité et d'une sécurité absolues quelles que soient les règles établies par le médecin biologiste parce qu'elles ne sont pas à l'abri de défaillances et que ces règles peuvent ne pas être respectées. La téléinformatique peut apporter dans ce domaine une rigueur beaucoup plus satisfaisante dans la mesure où, programmées, les règles imposées par un cahier des

charges aussi précis que possible sont fidèlement respectées. Il faut donc tâcher d'automatiser le plus possible les procédures. La mise à disposition des résultats sur un réseau type Minitel ou Videotex qui jusqu'à présent ne permettent pas le codage doit absolument être évitée. (33)

L'architecture du serveur doit être inconnue et inaccessible, même aux membres du personnel du laboratoire. (34)

Les critères suivants ne s'appliquent que dans le cas d'un serveur central contenant les données en consultation.

Les plages horaires de consultation doivent être limitées et secrètes. (35)

La communication doit être établie par le médecin, elle est suivie d'un rappel par le laboratoire: il est possible d'améliorer l'authentification en obligeant le serveur à rappeler le correspondant mais cette solution apporte pas mal de désagréments (le correspondant peut par exemple recevoir un autre appel au même moment). (36,37)

Une procédure automatique de déconnexion en cas de refus successifs du mot de passe et l'introduction d'un délai avant toute nouvelle tentative sont de nature à décourager les fraudeurs potentiels. (38,39)

B. Règlement de la banque de données

Toute banque de données médicales doit être soumise à un règlement reprenant:

- les finalités spécifiques de la banque
- les caractéristiques techniques y compris le cloisonnement des dossiers médicaux et les techniques de verrouillage
- les modalités d'accès
- les modalités de communication d'informations aux tiers et aux personnes concernées
- les mesures de sécurité concernant les données et les installations
- les conditions d'interconnexion avec d'autres banques de données
- les mesures de gestion prises pour assurer le respect de la déontologie médicale
- la procédure de délivrance des éléments sécurisants (cartes

à microprocesseur, par exemple)

- la gestion de la délivrance des permissions d'accès
- la gestion du renouvellement des éléments sécurisants après une certaine période ou lors d'une perte

La création d'une banque de données doit s'accompagner d'une information du public permettant à ceux dont les intérêts sont affectés de faire connaître leur point de vue.

Le règlement de la banque de données doit être soumis aux instances habilitées à contrôler le respect des principes déontologiques et à celles habilitées à contrôler le respect des principes essentiels de la protection des données et ce lors de la création mais aussi lors de toute modification du système.

C. Tableaux récapitulatifs et pondérations

Quatre pondérations sont possibles:

A=Indispensable

B=Hautement souhaitable

C=Souhaitable

D=Intéressant

1. Critères juridiques

	A	B	C	D
(1) Passage par l'Ordre des Médecins	X	.	.	.
(2) Finalité connue	.	.	X	.
(3) Finalité vérifiée	.	.	X	.
(4) Données adaptées à la finalité	X	.	.	.
(5) Durée de conservation non excessive	.	.	.	X
(6) Données obtenues et traitées loyalement et licitement	.	.	X	.
(7) Possibilité de consultation et de correction	.	.	.	X
(8) Données exactes et mises à jour	.	.	.	X
(9) Information des patients	X	.	.	.
(10) Consultation par plusieurs médecins traitants	.	.	X	.
(11) Possibilité de verrouillage	X	.	.	.
(12) Consentement écrit des personnes concernées pour le stockage	.	.	X	.
(13) Consentement écrit des personnes concernées pour la transmission	.	.	X	.
(14) Respect de la vie privée et du secret médical assuré par la confidentialité	.	.	X	.

2. Critères déontologiques

	A	B	C	D
(1) Standardisation au niveau du matériel	.	.	X	.
(2) Supervision par un médecin de l'Ordre des Médecins	.	.	X	.
(3) Validation par médecin biologiste	X	.	.	.
(4) Liberté de choix du patient	X	.	.	.
(5) Non constitution d'argument de choix	.	.	X	.
(6) Service non payant	X	.	.	.
(7) Passivité du serveur	X	.	.	.
(8) Le laboratoire exécutant est son propre serveur	X	.	.	.
(9) Pas de transmission directe des résultats du labo au patient	X	.	.	.
(10) Définition et limitation des conditions de transfert (consultation ou envoi)	X	.	.	.
(11) Pas de prise en charge des frais	X	.	.	.
(12) Nécessité de confirmation écrite	.	.	.	X
(13) Possibilité d'interdire globalement la transmission de certaines classes de résultats	.	X	.	.
(14) Cloisonnement des dossiers médicaux	X	.	.	.

3. Critères technologiques

	A	B	C	D
(1) Secours immédiat	.	.	.	X
(2) Systèmes redondants	.	.	X	.
(3) Réactions suite à une panne	.	X	.	.
(4) Fiabilité de la transmission des données	X	.	.	.
(5) Débits supportables par le réseau	X	.	.	.
(6) Compactage	.	.	X	.
(7) Simple et facile à mettre en oeuvre	.	X	.	.
(8) Connexion automatique	.	.	X	.
(9) Transmission transparente	.	.	X	.
(10) Chiffrement et déchiffrement transparents	.	.	X	.
(11) Compactage et décompactage transparents	.	.	X	.
(12) Coût minimum	.	.	X	.
(13) Possibilités d'extensions	.	X	.	.
(14) Standardisation du logiciel	.	.	.	X
(15) Standardisation du format d'échange	.	.	X	.
(16) Logiciels de qualité	.	X	.	.
(17) Matériel de qualité	.	X	.	.
(18) Mise en évidence de résultats anormaux	.	X	.	.
(19) Mention de la possibilité d'inexactitude	X	.	.	.
(20) Archivage des données	.	X	.	.
(21) Copie des données	.	X	.	.
(22) Archivage des messages	.	.	.	X
(23) Limitation de la durée	.	.	X	.
(24) Messages personnels	.	.	X	.
(25) Consultation obligatoire	.	X	.	.
(26) Plusieurs lignes	.	.	.	X
(27) Système de plages horaires	.	.	X	.
(28) Impression de messages sur papier	X	.	.	.
(29) Relevés statistiques	.	.	.	X

4. Critères sécuritaires

A B C D

(1) Spécification correcte de la politique de sécurité	X	.	.	.
(2) Environnement sécurisé	X	.	.	.
(3) Initialisation sécurisée du système	X	.	.	.
(4) Identification	X	.	.	.
(5) Identification par carte à microprocesseur	.	.	X	.
(6) Identification par caractéristique biologique	.	.	.	X
(7) Identification par code confidentiel et carte à microprocesseur	.	.	X	.
(8) Authentification	X	.	.	.
(9) Authentification par carte à microprocesseur	.	.	X	.
(10) Confidentialité sur la ligne par chiffrement	X	.	.	.
(11) Intégrité sur la ligne par chiffrement	X	.	.	.
(12) Chiffrement des messages	X	.	.	.
(13) Chiffrement des messages par la carte à microprocesseur	.	.	X	.
(14) Algorithme de chiffrement performant	.	X	.	.
(15) Algorithme de chiffrement bien utilisé	X	.	.	.
(16) Accès au réseau contrôlé	.	.	.	X
(17) Conservation des traces de transfert	X	.	.	.
(18) Enregistrement de la dernière demande de transfert	.	.	X	.
(19) Inventaire des matériels	.	X	.	.
(20) Non proximité des moyens de reproduction	.	X	.	.
(21) Protection contre la fuite illégale d'informations autorisées	.	X	.	.
(22) Vérification de l'adéquation du comportement de l'application aux spécifications	.	.	X	.
(23) Assurances	.	X	.	.
(24) Numéro d'appel privé	.	X	.	.
(25) Numéro d'appel secret	.	.	.	X
(26) Modification aisée des clés	X	.	.	.
(27) Modification des clés par l'autorité reconnue uniquement	.	X	.	.
(28) Identification certaine du malade	X	.	.	.
(29) Emploi de boîtes aux lettres	.	X	.	.
(30) Ordinateurs de transfert et ordinateur central physiquement séparés	.	.	.	X
(31) Institutions contrôlées par l'Etat	.	.	.	X
(32) Autorités publiques compétentes en matière de politique de soins de santé	.	.	.	X
(33) Automatisation de la procédure	.	.	X	.
(34) Architecture du serveur inconnue et inaccessible	.	.	.	X
(35) Heures d'appels limitées et secrètes	.	.	.	X
(36) Communication établie par le médecin	.	.	X	.
(37) Rappel par le laboratoire	.	.	.	X
(38) Procédure automatique de déconnexion	.	X	.	.
(39) Délai avant toute nouvelle tentative	.	X	.	.

D. Commentaires

Les critères juridiques et déontologiques ont, de par leur nature, un caractère impératif. Ils peuvent cependant devenir facultatifs soit parce qu'aucune contrainte légale n'existe, soit parce que l'application le permet.

Il n'y a pas, par exemple, d'obligation légale de communication de la finalité du système et donc à fortiori d'obligation de faire vérifier cette finalité (ce qui ne veut évidemment pas dire que cette vérification soit à rejeter). Il n'y a également aucune obligation de consentement écrit des personnes pour la transmission et le stockage des résultats. En ce qui concerne le stockage, le médecin n'a d'ailleurs pas le choix: il y est obligé par la loi.

S'agissant ici de résultats d'analyses médicales, c'est-à-dire essentiellement de mesures brutes, elles sont peu sensibles et peuvent être gardées de nombreuses années. Il est toutefois prudent de s'assurer qu'elles ne sont connues que par des personnes liées par le secret médical.

Il est difficilement concevable qu'un patient demande la consultation et la correction d'une mesure. En cas de doute, il demandera plus probablement une contre-expertise. Les données étant objectives, elles sont considérées comme exactes (à l'exactitude de la mesure près).

La consultation par plusieurs médecins traitants n'est pas strictement obligatoire. Il est en effet rare qu'un patient s'adresse simultanément à différents médecins si ce n'est pour des interventions bénignes et n'exigeant pas de suivi. La possibilité de changement occasionnel du médecin ayant droit de consultation des données est lui par contre absolument indispensable.

Les données communiquées ne sont pas considérées comme assez sensibles pour exiger le recours à des techniques de chiffrement performantes mais coûteuses. La confidentialité n'est assurée que par quelques transformations élémentaires.

Le système n'étant pas sensé être connecté à d'autres, la standardisation du matériel n'est pas indispensable.

La supervision du système par un médecin désigné à cet effet n'est peut-être pas la solution la plus adéquate. Ce médecin superviseur devrait connaître parfaitement les techniques employées pour pouvoir déceler toute infraction. Il doit donc atteindre un degré de connaissance que même beaucoup d'informaticiens n'ont pas. Il serait préférable que l'Ordre des Médecins désigne pour cette supervision un spécialiste en qui il a pleine confiance.

Il est difficilement concevable qu'un système performant de transmission des résultats ne constitue pas un argument de choix du la-

boratoire. Il ne faut toutefois pas tomber dans l'excès contraire et attacher une trop grande importance à cette capacité de transmission, négligeant les autres aspects (qualité de l'analyse, pertinence des résultats,...)

La possibilité d'interdire globalement la transmission de certaines classes de résultats est hautement souhaitable mais non indispensable si l'accès aux informations est bien réglementé et réservé à des personnes liées par le respect du secret médical.

La classification des critères technologiques et surtout sécuritaires est elle plus sujette à discussion: leur prise en compte est dépendante d'un niveau global à atteindre dans les domaines des performances, de la facilité d'emploi, de la sécurité et bien sûr du coût. Les préférences énoncées ci-dessus peuvent donc être remises en question suivant le ou les domaines mis en avant ou même suivant le moment considéré. Les deux premiers critères technologiques en sont une illustration: l'emploi de systèmes redondants apporte une très grande fiabilité technologique, la probabilité de pannes simultanées pour toutes les machines est extrêmement faible et, pour peu que des sauvegardes régulières soient faites, la reprise du travail en cours sur une autre machine ne pose guère de problèmes. On peut néanmoins lui préférer le recours à un secours immédiat (intervention - et non dépannage - en un certain laps de temps généralement exprimé en heures) qui a l'avantage de coûter nettement moins que l'achat d'un deuxième système. La baisse continue du prix du matériel peut remettre en cause ce raisonnement et ce d'autant plus qu'une deuxième machine peut servir à des tâches non prioritaires telles le traitement de textes, l'impression de graphiques,...

Les critères technologiques les plus importants me semblent être:

- la fiabilité de la transmission des données qui garantit la qualité des informations transmises: une erreur dans un nombre peut avoir des conséquences très dommageables
- dans le même ordre d'idées, le fait que des renseignements peuvent être inexacts par manque d'informations complètes et suffisamment récentes doit absolument être mentionné
- les débits doivent évidemment être supportables par le réseau ce qui ne pose dans la plupart des cas aucun problème, le volume de données n'étant jamais très important
- l'impression des messages sur papier permet au médecin d'être plus ou moins indépendant de la machine: il ne doit pas consulter l'ordinateur à chaque demande de renseignements.

La convivialité du système est à rechercher car il est destiné à être manipulé par des médecins qui ne sont pas toujours des spécialistes en informatique.

Le gestionnaire du système doit prévoir les réactions aux divers incidents possibles afin de prendre les mesures préventives permettant d'en atténuer les conséquences.

La standardisation du logiciel n'est que facultative car les applications sont pour la plupart locales. Une extension du système rendrait cette standardisation plus impérative.

Les relevés statistiques ne sont utiles qu'au technicien désireux de contrôler et de perfectionner le système. L'emploi de plusieurs lignes ne se justifie que si le trafic est assez important (rare).

La spécification complète et correcte des mesures de sécurité est absolument indispensable. Malheureusement elle est souvent réduite à une peau de chagrin (quand elle existe !) alors qu'elle constitue le pilier essentiel de la sécurité.

L'utilisation de codes confidentiels sera préférée à celles de cartes à microprocesseur essentiellement pour une raison de coût. Les cartes magnétiques, d'aspect extérieur similaire aux cartes à microprocesseur et de coût nettement moindre, n'offre pas plus de sécurité que les codes confidentiels.

Le réseau public étant employé, le chiffrement assurant la confidentialité et l'intégrité des messages est nécessaire. Mais plutôt que d'utiliser le nec plus ultra des systèmes de chiffrement - et donc aussi le plus cher - il faut s'attacher à utiliser correctement le système adéquat et surtout à en connaître les limites (durée de vie des clés entre autres).

Le laboratoire ou le cabinet médical étant considéré comme endroit sécurisé, il n'est pas nécessaire que le chiffrement se fasse au sein d'un boîtier sécurisé, il suffit que le message ne sorte jamais en clair du laboratoire ou du cabinet.

La conservation des traces de consultation est un des moyens les plus efficaces et malgré tout des meilleurs marchés pour avoir connaissance à posteriori d'une intrusion par une personne non autorisée.

V. Réalisations

A. Le système du Dr Beauloye

Un système de transmission de résultats d'analyses médicales entre un laboratoire et des médecins traitants est actuellement en développement au laboratoire du Dr Beauloye, à Moustier-sur-Sambre. Chaque médecin peut converser avec l'ordinateur serveur du laboratoire via un modem et le réseau téléphonique de la RTT.

1. Description du système

Deux ordinateurs physiquement séparés sont utilisés: un ordinateur central gérant le laboratoire et un ordinateur type PC pour les transferts de résultats.

Les demandes d'analyses sont introduites dans l'ordinateur central. Après traitement des échantillons et validation par le médecin biologiste, les résultats sont également introduits. Les données servent à l'édition de protocoles sur support papier et sur support magnétique (disquette au format IBM DOS).

Cette disquette permet le transfert des données sur le second ordinateur. Les fichiers de résultats de chaque patient sont compactés et chiffrés. Ils sont ensuite transférés dans la boîte aux lettres de chaque médecin traitant correspondant (cette boîte aux lettres est en fait un sous-répertoire).

Lorsque le médecin désire lire les données concernant ses patients, ils doit suivre une procédure bien précise. Il dispose d'une disquette d'appel qui contient

- le programme de communication
- les paramètres de la connexion: le numéro d'appel du serveur, les paramètres des modems,...
- un code (PIN) propre au médecin. Ce dernier est chiffré et permet après déchiffrement par le serveur de connaître le nom et le mot de passe du correspondant
- un code propre à l'ordinateur du médecin (la date de son système d'exploitation) ce qui l'oblige à toujours employer la même version du BIOS (partie en mémoire morte du système d'exploitation).
- une clé de déchiffrement sans laquelle il sera impossible au médecin de déchiffrer les données lui parvenant.

Le médecin lance le programme de connexion qui vérifie les paramètres de la connexion. Si ceux-ci sont corrects, la connexion est établie. Le code du médecin et le code de l'ordinateur sont

ensuite vérifiés. Le nom du médecin, la date et l'heure de l'appel sont enregistrés dans un fichier journal. Si tous ces codes sont corrects, le transfert des fichiers est permis. Lorsque les fichiers de résultats arrivent chez le médecin traitant, il doivent être déchiffrés (grâce à la clé de déchiffrement) et décompactés.

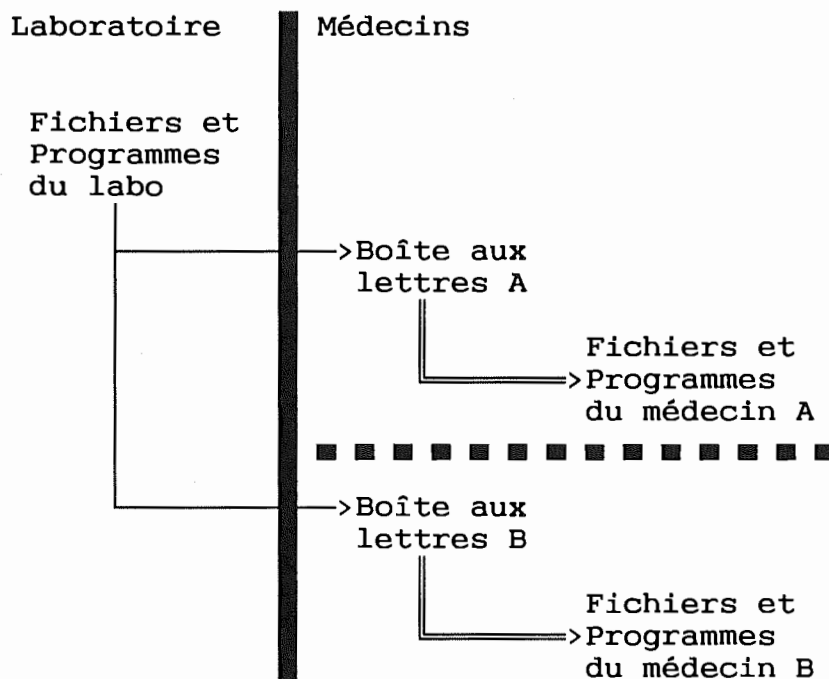
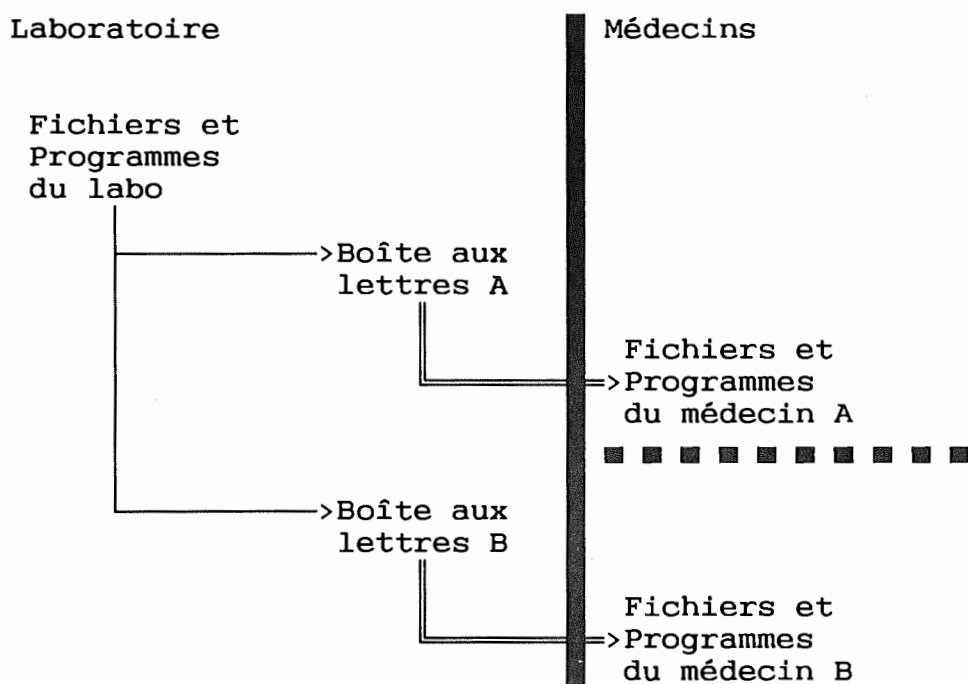
2. Système de boîtes aux lettres informatisées

Un système de boîtes aux lettres informatisées permet un cloisonnement des Dossiers médicaux (cfr III.A.4, IV.A.2)

Deux solutions peuvent être envisagées quant à l'emplacement des boîtes aux lettres informatisées:

- la boîte aux lettres est installée dans l'ordinateur du médecin. Le laboratoire peut y déposer le résultat d'une analyse (\rightarrow) mais ne peut y prélever quoi que ce soit. Le médecin peut lire le contenu de sa boîte et le transférer dans ses propres fichiers (\Rightarrow). Le laboratoire n'a accès qu'à la boîte aux lettres de son correspondant et non à ses autres données. Le médecin ne peut que recevoir des résultats.

- une série de boîtes aux lettres sont installées dans l'ordinateur du laboratoire. Le laboratoire peut y enregistrer le résultat d'une analyse (\rightarrow). Le médecin peut accéder à sa boîte aux lettres personnelle et prélever les résultats qui l'intéressent (\Rightarrow). Il n'a accès qu'à sa boîte personnelle. Le laboratoire est donneur passif et n'a aucun moyen d'entrer dans l'ordinateur du médecin.

Première solutionDeuxième solution

3. Réglementation

L'accès aux données est réglementé, le médecin ne peut prendre connaissance que des résultats concernant ses patients. La participation au système implique l'acceptation d'un règlement édité par le laboratoire. Cette participation n'est aucunement obligatoire. Le seul but du système est une communication meilleure et plus rapide du résultat de laboratoire validé par le biologiste ⁽¹⁾. Le règlement garantit la préservation du secret médical, le libre choix du patient et la liberté et l'indépendance du médecin.

a. La préservation du secret médical

La seule liaison entre l'ordinateur central et l'ordinateur de transfert est la disquette contenant les protocoles. Seuls les résultats des patients ayant permis la transmission y sont repris. Les fichiers stockés sur le serveur sont chiffrés.

Le serveur a toujours un rôle passif. Il ne sait lire les données contenues dans le système du médecin traitant.

L'initialisation du système ne peut être faite que par le médecin biologiste.

Le médecin ne peut lire que les fichiers stockés dans sa boîte aux lettres. Le numéro de téléphone du serveur est inconnu de l'appelant. Le temps de connexion est limité et les heures de fonctionnement du serveur sont confidentielles. Les différents codes d'accès sont aisément modifiables par le laboratoire et uniquement par lui. Ils le sont en cas de vol ou perte d'une disquette d'appel ou de tentatives d'intrusions.

b. Le libre choix du patient

Le patient a le choix du laboratoire et du mode de transmission des résultats de l'examen. Il est averti soit par le praticien, soit par le biologiste de l'existence du système de transmission ⁽¹⁾. Le logiciel du laboratoire rend possible l'interdiction du transfert des résultats des patients en ayant exprimé le désir.

c. La liberté et l'indépendance du médecin

Le médecin généraliste reste maître de sa décision d'informatiser la gestion de son cabinet médical. Le laboratoire n'intervient ni dans le choix, ni dans l'achat du matériel et/ou du logiciel ⁽¹⁾.

⁽¹⁾ Extrait du règlement du Dr Beauloye

B. Le système COBRA PC FAX

1. Description générale

L'utilisation de réseaux de communication et de réseaux locaux rend nécessaire une protection de bout en bout des informations. La MBLE - Secure Office Communication propose une solution qui apporte toute la sécurité voulue pour l'ordinateur et les applications de communication et est compatible avec les systèmes d'exploitation et/ou les applications standards.

COBRA-MAIL (Communications and Operations in BRANCH offices) représente une série de produits destinés à la transmission dans le domaine commercial de données, d'images et de sons. Dans cette gamme, COBRA-PC-FAX est un système de courrier électronique reliant deux PC et permettant la transmission de données et d'images, les deux PC étant connectés via le réseau téléphonique, un réseau local (LAN - Local Area Network) ou un réseau étendu (WAN - Wide Area Network). La communication est également possible avec tout fax de groupe 3.

La solution COBRA-PC-FAX est développée de telle manière qu'elle tire avantage:

- des facilités du telefax: très répandu, il permet la transmission d'images et de textes, l'emploi d'une ligne téléphonique standard et la communication rapide et à faible coût
- des commodités des PC: ordinateur décentralisé, universel, facile à utiliser, permettant un vaste choix de logiciels performants pour la manipulation de textes et d'images et une intégration de la fonction FAX dans le PC par une carte d'extension
- de concepts de sécurité d'avant-garde: contrôle d'accès et protection des données au moyen de la carte à microprocesseur, authentification des personnes et des messages, confidentialité par chiffrement, gestion des clés, emploi d'un système à clé publique.

COBRA - FAX est constitué de divers éléments:

- un ordinateur compatible AT et ses périphériques
- une carte PCFAX, carte d'extension remplissant toutes les fonctions de transmission et de réception des FAX ou d'autres fichiers PC
- des cartes à microprocesseur pour la protection et la conservation des clés
- un lecteur de cartes à microprocesseur, interne ou externe au

PC.

- le logiciel COBRA PC FAX, logiciel de sécurisation de documents. Ce logiciel peut être livré séparément et intégré à des procédures automatiques de bureautique

- le logiciel de personnalisation des cartes à microprocesseur. Ce logiciel n'est installé que sur certaines stations et est accompagné d'un guide de sécurité pour l'autorité. Les opérations de personnalisation réalisables sont:

- la modification des données non protégées, nom et autres données d'identification
- la remise en fonction d'une carte à microprocesseur bloquée
- la modification du code PIN
- la génération d'une copie d'une carte à microprocesseur détruite ou dont la durée de vie est dépassée

Ces opérations requièrent une carte à microprocesseur particulière appelée carte maître. La personnalisation peut être prise en charge par la MBLE ou par le client. Dans ce dernier cas, l'obtention des clés et leur archivage protégé chez le client est une excellente garantie pour la confidentialité de ces clés.

Il est également possible d'intégrer un réseau local à cette configuration, un logiciel spécifique gérant la sécurisation des documents au sein de ce réseau local.

Le module de chiffrement fonctionne de façon transparente, n'entraînant pas de modifications des équipements existants ou de leurs paramètres.

2. Comparaisons avec le telefax

Le telefax conventionnel souffre de quelques lacunes:

- aucun document confidentiel ne peut transiter sans plus
- les erreurs de destinataire n'empêchent pas l'impression du document chez celui-ci
- l'expéditeur du document n'est pas connu avec certitude
- aucune date officielle n'accompagne le document contrairement au télex et au courrier postal
- de l'information peut être ajoutée ou perdue

- l'accès au matériel est libre

L'intégration du telefax et de l'équipement de chiffrement en une carte PC FAX permet:

- la réception des messages en l'absence de l'opérateur autorisé: seule l'opération de déchiffrement requiert sa présence. Il n'est pas nécessaire de sécuriser les locaux
- une erreur de destinataire n'a pas de conséquence fâcheuse, même si celui-ci est un des membres du système, chacun ayant une clé de déchiffrement différente
- l'intégration des fonctionnalités et des documents du PC FAX aux applications du PC est facilitée
- un gain de temps: l'impression sur papier et la digitalisation ne sont plus nécessaires
- la création de documents FAX de haute qualité grâce aux performances graphiques des PC
- une réutilisation facile des FAX (édition, envoi à des tiers, ...)

3. Fonctionnalités

Les fonctionnalités du COBRA PC FAX peuvent être classées en trois catégories:

a. du point de vue des facilités

- envoi et réception de documents selon les normes téléfax T4 et T30 du CCITT
- tenue à jour d'une liste de destinataires et facilités de manipulations de cette liste
- rappel automatique en cas de problème sur la ligne
- envoi groupé de documents
- réception en tâche de fond, avertissement par signal sonore
- affichage de la liste des documents reçus et non encore traités
- rappel de documents stockés et traitements (rotation, extraction, addition,...)
- conversion de formats. Les formats reconnus sont les ASCII, WordPerfect, TIFF, MSP, PCX, CUT et ceux des images digita-

lisées par scanner

- paramétrisation: choix des périphériques (imprimantes, scanners, cartes d'adaptation graphique et type d'écrans), adaptation au réseau téléphonique, options de mise en page.

b. du point de vue de la sécurité

- initiative de l'échange réservée à l'expéditeur. Il est impossible de consulter à distance le contenu d'un dossier médical du laboratoire, la communication telefax ne permettant pas d'interaction. La seule information à contre-sens est le protocole T30. Il est aussi physiquement impossible au laboratoire de consulter les dossiers du médecin.

- confidentialité des messages grâce au chiffrement DES et des données stockées grâce à une clé personnelle. Chaque utilisateur a une clé secrète et une clé publique, la clé commune utilisée par le DES est générée grâce à l'algorithme de Diffie-Hellman. L'utilisation de clés différentes pour le chiffrement des messages d'une part et le chiffrement des données stockées d'autre part permet à une autorité reconnue de pouvoir déchiffrer les données d'un médecin sans mettre en péril le système de communication.

- intégrité des documents grâce à l'emploi du MAC, résumé produit au moyen d'une fonction à sens unique, protégée par une clé

- protection contre le rejeu

- authentification de la date et de l'heure de transmission et de réception par l'envoi d'une copie à un arbitre.

- non répudiation des envois.

Une journalisation des transactions concernant les données sensibles est le meilleur moyen de se protéger contre les attaques de personnes anonymes et les répudiations illicites de messages.

- intégrité des archives

- authentification des interlocuteurs

- authentification du terminal et de la carte d'accès

- séparation des domaines de responsabilité des gestionnaires de systèmes d'une part et des responsables de la sécurité

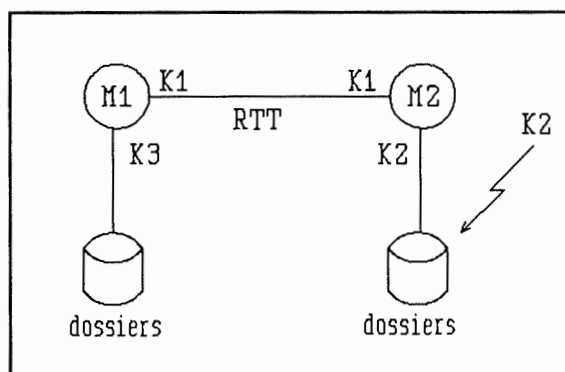


fig 14: Droit de regard de l'autorité

d'autre part. Le premier est responsable des machines et de leur fonctionnement normal, le second des informations stockées et de leur intégrité. On peut aussi définir un rôle d'arbitre pour la vérification des identités, des clés publiques et secrètes, du MAC, de la date et de l'heure, de l'accès, ... et un rôle d'autorité pour la génération et la distribution des clés. Ces deux rôles peuvent être combinés. La définition de rôles peut rendre plus facile certains contrôles, notamment par l'Ordre des Médecins.

c. du point de vue opérationnel

A ce niveau, les fonctionnalités sont essentiellement dues à l'emploi de la carte à microprocesseur. Dans la plupart des applications développées au SOC, la carte à microprocesseur de Philips est utilisée pour l'authentification des utilisateurs et la distribution sécurisée des clés de chiffrement.

- universalité: le système est valable pour tous les laboratoires grâce au principe des clés publiques: le libre choix du patient est garanti par la totale indépendance de la génération des paires clés publiques/clés privées par rapport au couple médecin/labo.

- authentification de la carte: vérification des clés de base du système

- refus de cartes volées ou de cartes reprises dans une liste noire grâce au rejet des clés publiques dans les systèmes les utilisant ou encore par reprogrammation de toutes les cartes avec de nouvelles clés (seule méthode dans le système à clé commune)

- transmission sécurisée, déchiffrement et vérification du code d'authentification rendus possibles seulement après présentation de la carte à microprocesseur et de son code PIN

- protection locale des archives par chiffrement au moyen d'une clé personnelle diversifiée grâce à une valeur aléatoire

- éjection automatique de la carte à microprocesseur après chaque chiffrement/déchiffrement afin d'éviter que quelqu'un ne tire profit d'une précédente action d'un opérateur pour chiffrer ou déchiffrer un autre document sans autorisation.

- possibilité de limitation du nombre d'accès à la carte et du nombre de présentations de PIN incorrects (cartes à durée de vie limitée)

- possibilité de changer le jeu de clés à un instant précis grâce à la présence de deux jeux dans la carte

Jeux: A, B, C,...

Carte série 1:

A	B
---	---

Carte série 2:

B	C
---	---

Durant la première année, le jeu A de la carte 1 est utilisé. Le premier janvier de la deuxième année, toutes les cartes passent au jeu B. Durant cette année les cartes 1 sont échangées contre des cartes 2 dont le jeu B est actif. Lorsque toutes les cartes ont été remplacées, on se retrouve dans la situation de départ. Si A, B et C sont différents, les cartes de la série 1 sont inutilisables à la fin de la deuxième année.

Note: une version de COBRA PC FAX existe sans carte à microprocesseur

C. Le système TRASEC

Le système TRASEC (TRANsmission SECurity) est un système sécurisé standard pour les transferts de fonds électroniques (EFT - Electronic Funds Transfert) entre les institutions financières et leurs clients. Ces institutions financières ont créé le C.I.R.I. (Centre for Interbank Research in Informatics). Le C.I.R.I. est une association de banques privées et publiques qui est responsable de la recherche, du développement, de la standardisation et de la maintenance de l'infrastructure informatique interbancaire, des projets et des applications.

Le système TRASEC est étudié ici alors que sa destination première ne correspond que très partiellement au problème qui nous occupe. On pourra ainsi évaluer une des démarches possibles qui est celle de transposer un système existant vers le milieu médical et d'éventuellement apporter certaines modifications à ce système. Les deux problèmes se ressemblent car il s'agit dans les deux cas d'échanges de données sensibles entre un "fournisseur" et un "client" et cela via des moyens de télécommunication, la différence la plus importante étant comme nous le verrons plus loin le besoin ou l'absence de besoin de confidentialité des données.

Après être passées des documents écrits et du contact visuel aux supports magnétiques (bandes, disques, cassettes,...), les institutions financières se servent des télécommunications pour effectuer les transferts.

L'introduction de l'informatique permet de:

- réduire le nombre d'opérations de routine (surtout administratives)
- assurer un meilleur service
- contrôler les coûts

Auparavant, l'authentification était assurée par une note accompagnatrice signée. Cette solution était peu efficace. Les responsables ont recherché une autre solution offrant plus de flexibilité tout en gardant un haut degré de sécurité et employant une procédure standard. Le C.I.R.I. a développé le système TRASEC dont les objectifs sont:

- la standardisation des procédures EFT garantissant l'indépendance d'un client vis-à-vis d'une banque particulière et la réutilisation du matériel investi
- un haut degré de sécurité c'est-à-dire
 - intégrité des données
 - authentification: l'identité de l'expéditeur doit être prouvée. Le processus d'authentification doit suppléer la signature manuelle qui est actuellement le seul mode légal. La technologie utilisée garantit l'unicité de la signature pour chacune des transactions et ce pour chaque mandataire
 - pas de chiffrement ou de confidentialité des données: le risque n'étant pas considéré comme assez important et les techniques cryptographiques n'étant pas jugées assez efficaces (en termes de coût/efficacité) pour une installation à grande échelle et manipulant de grands volumes de données
- l'intégration facile dans les systèmes informatiques et la convivialité par emploi de procédures automatisées
- l'indépendance vis-à-vis
 - des applications: transferts, domiciliations,...
 - des matériels: disques, bandes, cassettes, réseaux,...
 - des configurations des systèmes des clients et des banques
- une minimisation des coûts

Le système TRASEC a pour but de détecter les fraudes lors de la transmission et non lors de l'introduction de la transaction.

1. Description générale

a. Modularisation

Le système TRASEC est composé de deux modules: un module de condensation et un module d'authentification. Le module de condensation est contenu dans l'ordinateur de traitement des fichiers de données tandis que le module d'authentification est contenu dans un terminal. Le module de condensation est un programme qui, grâce à des permutations, des translations et des opérations ou-logique, condense un fichier donnant un résumé. Ce résumé protège l'intégrité du fichier et constitue l'entrée du module d'authentification. Le module d'authentification basé sur la carte à microprocesseur génère les signatures digitales. Il offre également un environnement sécurisé pour les procédures de chiffrement et les clés secrètes. Cette approche modulaire a plusieurs avantages:

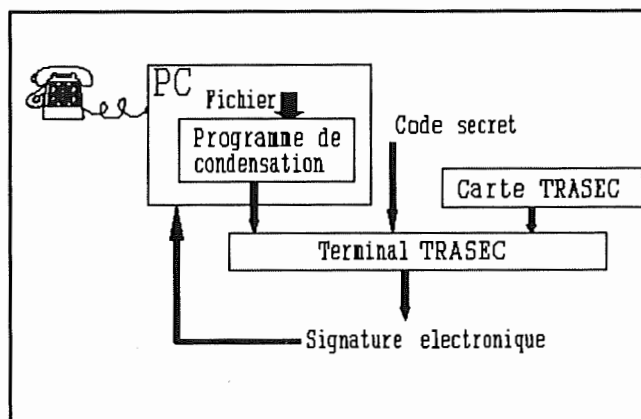


fig 15: Schéma du système TRASEC

Le module de condensation est un programme qui, grâce à des permutations, des translations et des opérations ou-logique, condense un fichier donnant un résumé. Ce résumé protège l'intégrité du fichier et constitue l'entrée du module d'authentification. Le module d'authentification basé sur la carte à microprocesseur génère les signatures digitales. Il offre également un environnement sécurisé pour les procédures de chiffrement et les clés secrètes. Cette approche modulaire a plusieurs avantages:

- une flexibilité fonctionnelle: on peut, par exemple, n'utiliser que le module de condensation assurant ainsi l'intégrité et faire accompagner le document d'une signature manuelle classique
- les clés secrètes sont à l'abri des regards indiscrets
- l'emploi d'un résumé au lieu du texte complet en entrée du module d'authentification améliore le temps de réponse du module

b. Le module d'authentification

La signature digitale générée est une chaîne de caractères contenant de l'information chiffrée fonction de l'entrée et rendant possible l'identification de l'émetteur par le récepteur. Les arguments à l'entrée sont:

- le résumé produit du contenu du transfert (les données à protéger)
- la clé d'identification secrète de l'émetteur
- un numéro de séquence

Une signature digitale accompagne chaque transfert. Le même

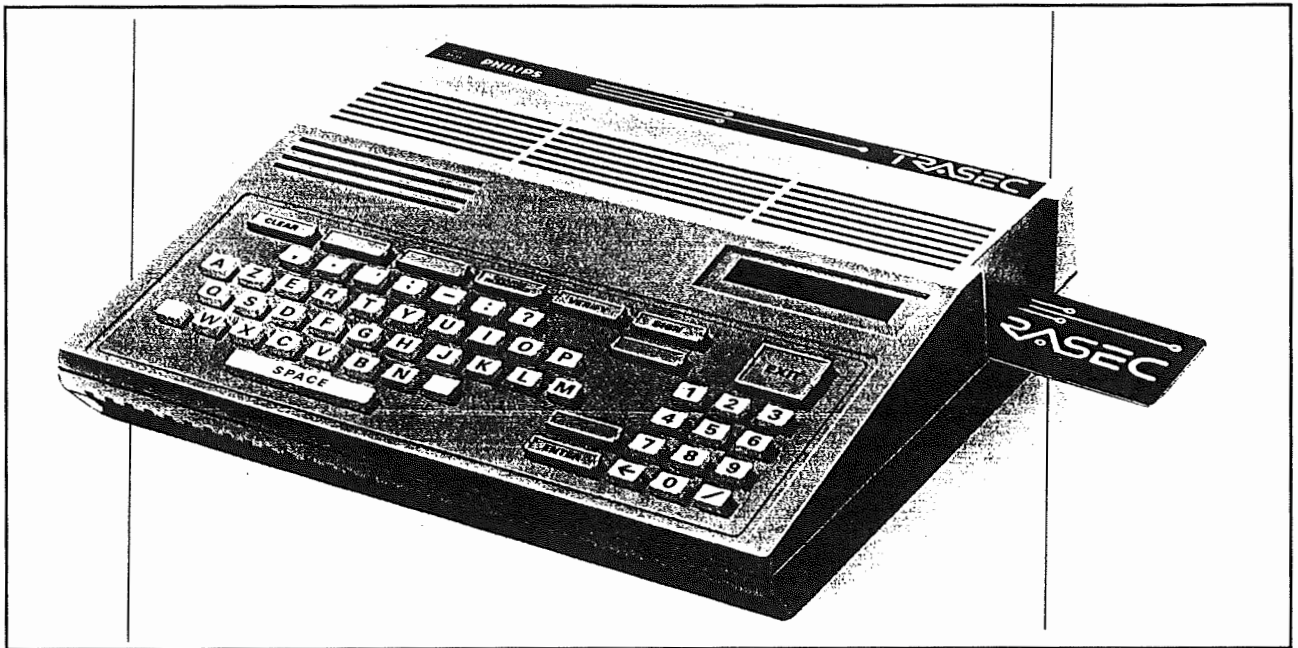


fig 16: Terminal TRASEC

calcul est effectué chez le destinataire qui si les deux signatures sont différentes peut en conclure que le message a été altéré ou que l'émetteur n'est pas le bon ou encore que l'ordre des messages a été modifié.

Il est actuellement communément admis que seuls les algorithmes de chiffrement standard sont acceptables:

- leur force réside dans le secret de la clé et non dans celui de l'algorithme
- la résistance aux attaques peut être évaluée par des organismes indépendants.

Le C.I.R.I. a choisi le DES en mode CBC (voir III.C.6.d.(3)), la signature digitale étant dérivée du dernier résultat de l'algorithme.

Les désavantages du DES par rapport au RSA sont réduits grâce à:

- une distribution aisée et sûre des clés. Les clés sont gardées dans une base de données spécialement protégée d'une part et dans une carte à microprocesseur d'autre part. Cette carte à microprocesseur est personnelle et le mot de passe est transmis par courrier séparé.
- une authentification irréfutable: la base de données des mots de passe est protégée de façon telle qu'il est impos-

sible à la banque de générer un message à la place d'un des clients.

c. La carte à microprocesseur

Le secret n'étant contenu que dans les clés, la sauvegarde de celui-ci dépend essentiellement de la façon dont elles sont gardées secrètes. La carte à microprocesseur (voir III.C.7.a) est une des meilleures solutions à ce problème: elle est relativement bon marché, sûre, conviviale et assez répandue. La carte à microprocesseur garantit que les clés ou les codes secrets ne la quitte jamais et que les processus ne peuvent être modifiés. L'EPROM contient les programmes et données propres à l'application TRASEC: clés d'authentification secrètes, mot de passe et nombre d'erreurs pour ce mot de passe, données d'identification, numéro de séquence.

d. La gestion des mots de passe

Un premier code secret est transmis dans une enveloppe spéciale. A la première manipulation, la carte invite l'utilisateur à choisir un autre code de 6 à 12 caractères. Ce code secret, strictement personnel et pouvant être modifié à plusieurs reprises, donne accès aux fonctions de la carte. La validation du mot de passe est obligatoire pour l'exécution des autres fonctions. Après trois erreurs d'introduction de code consécutives, la carte se bloque la protégeant ainsi de toute utilisation frauduleuse. Le risque en cas de perte ou vol est donc fortement diminué.

e. Le terminal TRASEC

Le terminal TRASEC se compose d'un lecteur de cartes à microprocesseur, d'un clavier et d'un écran. Après introduction de la carte, apparaissent à l'écran des instructions invitant à introduire le code secret et les données de la transaction. A l'issue du traitement de ces données, la signature électronique apparaît à l'écran. Grâce à ce dialogue convivial, le titulaire de la carte n'éprouve aucune difficulté pour exécuter les fonctions telles que signature, modification du code secret,... Un terminal par entreprise suffit pour authentifier toutes les transactions avec n'importe quel institution financière adhérant au système TRASEC.

f. La validation et la génération de cartes

Chaque banque dispose d'équipements permettant la validation des signatures digitales reçues et l'initiation de nouvelles cartes.

Un ordinateur personnel assure un haut niveau de sécurité grâce à une carte enfichée dans le PC et contenant un pro-

cesseur DES qui:

- recalcule la signature digitale et la compare avec celle reçue
- chiffre le système d'exploitation, le logiciel d'application et les données stockées sur disque

L'accès au PC est contrôlé par la carte à microprocesseur contenant les privilèges de l'opérateur.

D. Evaluation de la solution du Dr Beauloye

Trois réponses sont possibles:

O=Le critère est satisfait

N=Le critère n'est pas satisfait

--=Le critère n'est pas pertinent

1. Critères juridiques

Passage par l'Ordre des Médecins	O (1)
Finalité connue	O
Finalité vérifiée	N (2)
Données adaptées à la finalité	O (3)
Durée de conservation non excessive	- (4)
Données obtenues et traitées loyalement et licitement	O (5)
Possibilité de consultation et de correction	N (6)
Données exactes et mises à jour	- (7)
Information des patients	N (8)
Consultation par plusieurs médecins traitants	O (9)
Possibilité de verrouillage	N
Consentement écrit des personnes concernées pour le stockage	N
Consentement écrit des personnes concernées pour la transmission	N
Respect de la vie privée et du secret médical assuré par la confidentialité	N

(1) L'Ordre des Médecins de la province de Namur a marqué son accord pour l'utilisation du système

(2) La vérification doit être faite par l'Ordre des Médecins

(3) Les données sont définies par le laboratoire du Docteur Beauloye

(4) La durée de conservation des données n'est pas précisée

(5) Les données n'étant que le résultat de ses mesures, une obtention illicite par le laboratoire est impensable

(6) Un résultat d'analyse n'est pas considéré comme donnée assez sensible pour justifier une possibilité de correction

(7) Dans le cadre du laboratoire, elles sont considérées comme correctes et non amendables

(8) Ne s'agissant ici que de données techniques (résultats d'analyses), le patient est tenu à l'écart de la démarche

(9) Il suffit d'envoyer les résultats à chacun de ces médecins

2. Critères déontologiques

Standardisation au niveau du matériel	O (1)
Supervision par un médecin de l'Ordre des Médecins	N (2)
Validation par médecin biologiste	O (3)
Liberté de choix du patient	N
Non constitution d'argument de choix	N
Service non payant	O
Passivité du serveur	O
Le laboratoire exécutant est son propre serveur	O
Pas de transmission directe des résultats du labo au patient	O
Définition et limitation des conditions de transfert (consultation ou envoi)	N
Pas de prise en charge des frais	O
Nécessité de confirmation écrite	N (4)
Possibilité d'interdire globalement la transmission de certaines classes de résultats	N
Cloisonnement des dossiers médicaux	O (5)

(1) Emploi de PC

(2)

(3) Les résultats sont stockés dans l'ordinateur central du laboratoire. Ce sont ces résultats qui servent à l'impression du protocole validé par le médecin biologiste et au transfert vers l'ordinateur serveur

(4) Par confirmation écrite, on entend une confirmation par la voie habituelle. Une telle confirmation enlèverait quasiment tout intérêt au système (coût prohibitif). Il faut cependant, pour assurer la validation, produire une copie locale

(5) Par le laboratoire

3. Critères technologiques

Secours immédiat	N ⁽¹⁾
Systèmes redondants	N ⁽¹⁾
Réactions suite à une panne	N
Fiabilité de la transmission des données	O ⁽²⁾
Débits supportables par le réseau	O
Compactage	O
Simple et facile à mettre en oeuvre	O
Connexion automatique	O
Transmission transparente	N
Chiffrement et déchiffrement transparents	N
Compactage et décompactage transparents	N
Coût minimum	O
Possibilités d'extensions	O ⁽³⁾
Standardisation du logiciel	N
Standardisation du format d'échange	N
Logiciels de qualité	N
Matériel de qualité	O
Mise en évidence de résultats anormaux	N ⁽⁴⁾
Mention de la possibilité d'inexactitude	N ⁽⁴⁾
Archivage des données	O
Copie des données	N
Archivage des messages	O ⁽⁵⁾
Limitation de la durée	O
Messages personnels	N ⁽⁴⁾
Consultation obligatoire	N ⁽⁴⁾
Plusieurs lignes	N ⁽⁶⁾
Système de plages horaires	O
Impression de messages sur papier	O
Relevés statistiques	N

⁽¹⁾ Le laboratoire peut permettre une interruption plus ou moins longue du service de transmission, les résultats étant alors transmis par voie habituelle

⁽²⁾ Grâce au protocole XModem

⁽³⁾ Ce sont celles du monde des PC

⁽⁴⁾ Ces fonctionnalités doivent être prises en charge par le logiciel de composition du document

⁽⁵⁾ Une journalisation des messages est possible

⁽⁶⁾ La densité du trafic ne le justifie pas

4. Critères sécuritaires

Spécification correcte de la politique de sécurité	O ⁽¹⁾
Environnement sécurisé	N
Initialisation sécurisée du système	N
Identification	O
Identification par carte à microprocesseur	N
Identification par caractéristique biologique	N
Identification par code confidentiel et carte à microprocesseur	N
Authentification	O
Authentification par carte à microprocesseur	N
Confidentialité sur la ligne par chiffrement	O
Intégrité sur la ligne par chiffrement	O
Chiffrement des messages	O
Chiffrement des messages par la carte à microprocesseur	N
Algorithme de chiffrement performant	N
Algorithme de chiffrement bien utilisé	N
Accès au réseau contrôlé	O
Conservation des traces de transfert	O
Enregistrement de la dernière demande de transfert	N
Inventaire des matériels	N
Non proximité des moyens de reproduction	N
Protection contre la fuite illégale d'informations autorisées	O
Vérification de l'adéquation du comportement de l'application aux spécifications	N ⁽²⁾
Assurances	N
Numéro d'appel privé	O
Numéro d'appel secret	O
Modification aisée des clés	O
Modification des clés par l'autorité reconnue uniquement	O
Identification certaine du malade	N ⁽³⁾
Emploi de boîtes aux lettres	O
Ordinateurs de transfert et ordinateur central physiquement séparés	O
Institutions contrôlées par l'Etat	N
Autorités publiques compétentes en matière de politique de soins de santé	N
Automatisation de la procédure	N
Architecture du serveur inconnue et inaccessible	N
Heures d'appels limitées et secrètes	O
Communication établie par le médecin	O
Rappel par le laboratoire	N
Procédure automatique de déconnexion	O
Délai avant toute nouvelle tentative	O

⁽¹⁾ Cette spécification doit se faire en collaboration avec l'Ordre des Médecins

- (²) Pas de spécifications, ni d'organisme contrôleur indépendant
- (³) Ces fonctionnalités doivent être prises en charge par le logiciel de composition du document

E. Evaluation de la solution MBLE

Trois réponses sont possibles:

O=Le critère est satisfait

N=Le critère n'est pas satisfait

--=Le critère n'est pas pertinent

1. Critères juridiques

Passage par l'Ordre des Médecins	O (1)
Finalité connue	- (2)
Finalité vérifiée	- (3)
Données adaptées à la finalité	- (4)
Durée de conservation non excessive	- (5)
Données obtenues et traitées loyalement et licitement	O (6)
Possibilité de consultation et de correction	N (7)
Données exactes et mises à jour	- (8)
Information des patients	N (9)
Consultation par plusieurs médecins traitants	O (10)
Possibilité de verrouillage	N
Consentement écrit des personnes concernées pour le stockage	N
Consentement écrit des personnes concernées pour la transmission	N
Respect de la vie privée et du secret médical assuré par la confidentialité	O (11)

(1) La MBLE a entrepris les démarches à l'Ordre des Médecins

(2) Une acceptation par l'Ordre des Médecins sera certainement subordonnée à une définition précise de la finalité

(3) La vérification doit être faite par l'Ordre des Médecins

(4) Les données ne sont pas définies par la MBLE. Elles devraient plutôt l'être par l'Ordre des Médecins

(5) La durée de conservation des données n'est pas précisée. Cette caractéristique d'ordre organisationnel doit être imposée par l'Ordre des Médecins.

(6) Les données n'étant que le résultat de ses mesures, une obtention illicite par le laboratoire est impensable

(7) Un résultat d'analyse n'est pas considéré comme donnée assez sensible pour justifier une possibilité de correction

(8) Dans le cadre du laboratoire, elles sont considérées comme correctes et non amendables

(9) Ne s'agissant ici que de données techniques (résultats d'analyses), le patient est tenu à l'écart de la démarche

(10) Il suffit d'envoyer les résultats à chacun de ces médecins

(11) Grâce au chiffrement des données

2. Critères déontologiques

Standardisation au niveau du matériel	O (1)
Supervision par un médecin de l'Ordre des Médecins	N (2)
Validation par médecin biologiste	O (3)
Liberté de choix du patient	O (4)
Non constitution d'argument de choix	O (4)
Service non payant	O
Passivité du serveur	N (5)
Le laboratoire exécutant est son propre serveur	O
Pas de transmission directe des résultats du labo au patient	O
Définition et limitation des conditions de transfert (consultation ou envoi)	N (6)
Pas de prise en charge des frais	O
Nécessité de confirmation écrite	N (7)
Possibilité d'interdire globalement la transmission de certaines classes de résultats	N (8)
Cloisonnement des dossiers médicaux	O (9)

(1) Emploi de PC et de la norme Telefax

(2) Le rôle de l'Ordre des Médecins et de ses mandataires n'est pas encore défini

(3) Par emploi de la carte à microprocesseur personnelle

(4) Grâce à la standardisation Telefax

(5) C'est en fait le récepteur qui est passif

(6) Il n'y a actuellement pas de possibilité de hiérarchiser les accès

(7) Par confirmation écrite, on entend une confirmation par la voie habituelle. Une telle confirmation enlèverait quasiment tout intérêt au système (coût prohibitif)

(8) Cette interdiction doit être prise en charge par le logiciel de composition du document

(9) Par le laboratoire

3. Critères technologiques

Secours immédiat	N ⁽¹⁾
Systèmes redondants	N ⁽¹⁾
Réactions suite à une panne	N
Fiabilité de la transmission des données	O ⁽²⁾
Débits supportables par le réseau	O
Compactage	N
Simple et facile à mettre en oeuvre	O ⁽³⁾
Connexion automatique	O ⁽³⁾
Transmission transparente	N ⁽⁴⁾
Chiffrement et déchiffrement transparents	O ⁽⁵⁾
Compactage et décompactage transparents	-
Coût minimum	N
Possibilités d'extensions	O ⁽⁶⁾
Standardisation du logiciel	O
Standardisation du format d'échange	O ⁽⁷⁾
Logiciels de qualité	O
Matériel de qualité	O
Mise en évidence de résultats anormaux	N ⁽⁸⁾
Mention de la possibilité d'inexactitude	N ⁽⁸⁾
Archivage des données	O ⁽⁹⁾
Copie des données	N
Archivage des messages	-
Limitation de la durée	N
Messages personnels	N ⁽⁸⁾
Consultation obligatoire	N ⁽⁸⁾
Plusieurs lignes	N
Système de plages horaires	-
Impression de messages sur papier	O
Relevés statistiques	N

⁽¹⁾ Le laboratoire peut permettre une interruption plus ou moins longue du service de transmission, les résultats étant alors transmis par voie habituelle

⁽²⁾ Grâce au protocole Telefax

⁽³⁾ Essentiellement grâce au caractère professionnel du logiciel

⁽⁴⁾ Il n'est actuellement pas prévu d'intégrer le programme de communication à un logiciel de traitement de dossiers par exemple. La conception modulaire du programme devrait cependant permettre une intégration sans trop de difficultés

⁽⁵⁾ Dès qu'ils sont sélectionnés (une fois pour toutes) les chiffrement et déchiffrement se font automatiquement

⁽⁶⁾ Ce sont celles du monde des PC

⁽⁷⁾ Il s'agit ici des formats physiques (WordPerfect, formats graphiques TIFF, PCX, MSP, ...) et non des formats logiques

⁽⁸⁾ Ces fonctionnalités doivent être prises en charge par le logiciel de composition du document

⁽⁹⁾ Par stockage des messages échangés dans le PC

4. Critères sécuritaires

Spécification correcte de la politique de sécurité	- (1)
Environnement sécurisé	O (2)
Initialisation sécurisée du système	O (3)
Identification	O
Identification par carte à microprocesseur	O
Identification par caractéristique biologique	N
Identification par code confidentiel et carte à microprocesseur	O
Authentification	O
Authentification par carte à microprocesseur	O
Confidentialité sur la ligne par chiffrement	O
Intégrité sur la ligne par chiffrement	O
Chiffrement des messages	O
Chiffrement des messages par la carte à microprocesseur	O
Algorithme de chiffrement performant	O
Algorithme de chiffrement bien utilisé	O
Accès au réseau contrôlé	O
Conservation des traces de transfert	N
Enregistrement de la dernière demande de transfert	N
Inventaire des matériels	-
Non proximité des moyens de reproduction	-
Protection contre la fuite illégale d'informations autorisées	-
Vérification de l'adéquation du comportement de l'application aux spécifications	N (4)
Assurances	-
Numéro d'appel privé	-
Numéro d'appel secret	-
Modification aisée des clés	O (5)
Modification des clés par l'autorité reconnue uniquement	O
Identification certaine du malade	N (6)
Emploi de boîtes aux lettres	O
Ordinateurs de transfert et ordinateur central physiquement séparés	N (7)
Institutions contrôlées par l'Etat	N
Autorités publiques compétentes en matière de politique de soins de santé	N
Automatisation de la procédure	N (8)
Architecture du serveur inconnue et inaccessible	N
Heures d'appels limitées et secrètes	-
Communication établie par le médecin	-
Rappel par le laboratoire	-
Procédure automatique de déconnexion	N
Délai avant toute nouvelle tentative	-

- (¹) Cette spécification doit se faire en collaboration avec l'Ordre des Médecins
- (²) La sécurisation des locaux n'est pas nécessaire, les données étant chiffrées
- (³) Grâce à la carte à microprocesseur
- (⁴) Pas de spécifications, ni d'organisme contrôleur indépendant
- (⁵) Par échange de cartes à microprocesseur
- (⁶) Ces fonctionnalités doivent être prises en charge par le logiciel de composition du document
- (⁷) Le caractère unidirectionnel de la transmission rend cette précaution inutile
- (⁸) La procédure est toujours initiée manuellement

F. Evaluation de la solution TRASEC

Trois réponses sont possibles:

O=Le critère est satisfait

N=Le critère n'est pas satisfait

=Le critère n'est pas pertinent

1. Critères juridiques

Passage par l'Ordre des Médecins	- (1)
Finalité connue	- (1)
Finalité vérifiée	- (1)
Données adaptées à la finalité	- (1)
Durée de conservation non excessive	- (1)
Données obtenues et traitées loyalement et licitement	- (1)
Possibilité de consultation et de correction	- (1)
Données exactes et mises à jour	- (1)
Information des patients	- (1)
Consultation par plusieurs médecins traitants	- (1)
Possibilité de verrouillage	- (1)
Consentement écrit des personnes concernées pour le stockage	- (1)
Consentement écrit des personnes concernées pour la transmission	- (1)
Respect de la vie privée et du secret médical assuré par la confidentialité	- (1)

(1) Le système TRASEC a été conçu pour effectuer des transactions sécurisées entre institutions financières. L'étude de sa transposition en milieu médical n'a pas encore été faite. Il est donc prématuré de l'évaluer selon ces critères.

2. Critères déontologiques

Standardisation au niveau du matériel	O (1)
Supervision par un médecin de l'Ordre des Médecins	- (2)
Validation par médecin biologiste	- (2)
Liberté de choix du patient	O (3)
Non constitution d'argument de choix	O (3)
Service non payant	N (4)
Passivité du serveur	N (5)
Le laboratoire exécutant est son propre serveur	O
Pas de transmission directe des résultats du labo au patient	O
Définition et limitation des conditions de transfert (consultation ou envoi)	- (2)
Pas de prise en charge des frais	- (2)
Nécessité de confirmation écrite	N (6)
Possibilité d'interdire globalement la transmission de certaines classes de résultats	- (7)
Cloisonnement des dossiers médicaux	O (8)

(1) Emploi de PC et de terminaux standards

(2) Le système TRASEC a été conçu pour effectuer des transactions sécurisées entre institutions financières. L'étude de sa transposition en milieu médical n'a pas encore été faite. Il est donc prématuré de l'évaluer selon ces critères.

(3) Grâce à la standardisation du matériel

(4) Le service TRASEC est payant: la location est de 250F par mois. Une caution de 5000F est demandée par terminal

(5) C'est en fait le récepteur qui est passif

(6) Par confirmation écrite, on entend une confirmation par la voie habituelle. Une telle confirmation enlèverait quasiment tout intérêt au système (coût prohibitif)

(7) Cette interdiction doit être prise en charge par le logiciel de composition du document

(8) Par le laboratoire

3. Critères technologiques

Secours immédiat	N ⁽¹⁾
Systèmes redondants	N ⁽¹⁾
Réactions suite à une panne	N
Fiabilité de la transmission des données	O
Débits supportables par le réseau	O
Compactage	N
Simple et facile à mettre en oeuvre	O ⁽²⁾
Connexion automatique	O ⁽²⁾
Transmission transparente	N ⁽³⁾
Chiffrement et déchiffrement transparents	-
Compactage et décompactage transparents	-
Coût minimum	O
Possibilités d'extensions	O ⁽⁴⁾
Standardisation du logiciel	O
Standardisation du format d'échange	N
Logiciels de qualité	O
Matériel de qualité	O
Mise en évidence de résultats anormaux	N ⁽⁵⁾
Mention de la possibilité d'inexactitude	N ⁽⁵⁾
Archivage des données	N
Copie des données	N
Archivage des messages	N
Limitation de la durée	N
Messages personnels	N ⁽⁵⁾
Consultation obligatoire	N ⁽⁵⁾
Plusieurs lignes	N
Système de plages horaires	-
Impression de messages sur papier	O
Relevés statistiques	N

⁽¹⁾ Le laboratoire peut permettre une interruption plus ou moins longue du service de transmission, les résultats étant alors transmis par voie habituelle

⁽²⁾ Essentiellement grâce au caractère professionnel du logiciel

⁽³⁾ Il n'est actuellement pas prévu d'intégrer le programme de communication à un logiciel de traitement de dossiers par exemple

⁽⁴⁾ Ce sont celles du monde des PC

⁽⁵⁾ Ces fonctionnalités doivent être prises en charge par le logiciel de composition du document

4. Critères sécuritaires

Spécification correcte de la politique de sécurité	- (1)
Environnement sécurisé	N
Initialisation sécurisée du système	N
Identification	O
Identification par carte à microprocesseur	O
Identification par caractéristique biologique	N
Identification par code confidentiel et carte à microprocesseur	O
Authentification	O
Authentification par carte à microprocesseur	O
Confidentialité sur la ligne par chiffrement	N
Intégrité sur la ligne par chiffrement	O
Chiffrement des messages	N
Chiffrement des messages par la carte à microprocesseur	N
Algorithme de chiffrement performant	-
Algorithme de chiffrement bien utilisé	-
Accès au réseau contrôlé	O
Conservation des traces de transfert	N
Enregistrement de la dernière demande de transfert	N
Inventaire des matériels	-
Non proximité des moyens de reproduction	-
Protection contre la fuite illégale d'informations autorisées	-
Vérification de l'adéquation du comportement de l'application aux spécifications	- (2)
Assurances	-
Numéro d'appel privé	-
Numéro d'appel secret	-
Modification aisée des clés	O (3)
Modification des clés par l'autorité reconnue unique-ment	O
Identification certaine du malade	N (4)
Emploi de boîtes aux lettres	N
Ordinateurs de transfert et ordinateur central physiquement séparés	N
Institutions contrôlées par l'Etat	N
Autorités publiques compétentes en matière de politique de soins de santé	N
Automatisation de la procédure	N (5)
Architecture du serveur inconnue et inaccessible	N
Heures d'appels limitées et secrètes	-
Communication établie par le médecin	-
Rappel par le laboratoire	-
Procédure automatique de déconnexion	N
Délai avant toute nouvelle tentative	-

(1) Cette spécification doit se faire en collaboration avec l'Ordre des Médecins

- (²) Pas de spécifications, ni d'organisme contrôleur indépendant
- (³) Par échange de cartes à microprocesseur
- (⁴) Ces fonctionnalités doivent être prises en charge par le logiciel de composition du document
- (⁵) La procédure est toujours initiée manuellement

VI. Conclusions

La définition de critères peut se faire de deux manières assez différentes:

- par étude théorique du contexte: étude des facteurs juridiques, de la déontologie, des technologies et de la sécurité sans se soucier du problème particulier
- par observation de systèmes à tester.

La première méthode permet d'obtenir des critères objectifs mais parfois trop généraux et non applicables au cas particulier qui nous occupe (le critère de la durée de conservation des données en est un bon exemple). Cette démarche, plus sérieuse car plus objective, est cependant plus ardue car elle requiert une connaissance en profondeur des domaines correspondants. Poussée à l'extrême, elle débouche sur l'écriture de documents tels l'Information Technology Security Evaluation Criteria [ITS]. Ces documents ne sont dans la plupart des cas exploitables que par des spécialistes.

La seconde méthode permet de dégager des critères "collant" bien au problème mais dont la prise en compte dépend de leur mise en évidence pour au moins une des solutions testées. De plus, de tels critères ne sont pas toujours applicables à toutes les solutions. On a alors aussi tendance à privilégier certains aspects et le danger d'oublier certaines parties essentielles est assez grand.

J'ai dans ce mémoire employé les deux méthodes: après avoir étudié les différents domaines (trop superficiellement sans doute), j'ai tenté de trouver le plus de critères objectifs possible. J'ai ensuite étudié différentes solutions et ai progressivement enrichi l'ensemble des critères.

Pour chacun de ces critères une appréciation ou note partielle NP est donnée (V.D à V.F).

Le problème qui se pose alors est la comparaison globale des solutions, ou en d'autres mots la composition des notes partielles (NP) en une note globale (NG).

En toute généralité, on a: $NG = f(NP's)$, la difficulté résidant précisément dans la détermination de cette fonction f. L'importance des critères étant inégale, une pondération leur est appliquée (IV.C). Il faudrait également tenir compte du fait que certains critères ne sont pas indépendants (dans la comparaison ci-dessous, cette dépendance entre critères n'a pas été prise en compte).

Une des agrégations possibles (sans doute la plus simple) pourrait être la suivante:

- une pondération de

4	est associée à un critère dont la satisfaction est indispensable
3	hautement souhaitable
2	souhaitable
1	superflue

- cette pondération est multipliée par +1 si le critère est satisfait, par -1 s'il ne l'est pas et par 0 si le critère n'est pas applicable.

Exemple: pour la solution du Dr Beauloye, le premier critère (Passage par l'Ordre des Médecins) reçoit une note partielle de $4*(+1) = 4$, le troisième (Finalité vérifiée) une note partielle de $2*(-1) = -2$.

- les différentes notes partielles sont, pour un même domaine (juridique, déontologique, technologique et sécuritaire), sommées donnant quatre notes globales permettant d'apprécier la solution plus ... globalement.

On obtient alors les résultats suivants:

	Beauloye	Cobra-PC-Fax	Trasec
Juridique	-2	-3	0
Déontologique	14	18	11
Technologique	0	3	-6
Sécuritaire	9	32	-17

Si pour les trois premiers domaines, les trois solutions se tiennent d'assez près (avec un léger désavantage pour la troisième), il n'en est pas de même pour le quatrième domaine. La solution Trasec présente de nombreuses lacunes tandis que la solution Cobra-PC-Fax est très performante, la solution du Dr Beauloye s'en tirant avec tous les honneurs sachant qu'il ne s'agit là que d'une solution "amateur" (par opposition au caractère professionnel des deux autres solutions).

Un aspect important du problème n'a pas été évoqué: celui du coût. Il est souvent déterminant dans le choix d'une solution. La solution du Dr Beauloye ne coûte pratiquement rien tandis qu'à l'autre extrême, la solution Cobra-PC-Fax coûte approximativement 150000 F par station, la solution Trasec se situant entre les deux (250 F par mois et par station + 5000 F de caution par terminal).

La tentative d'évaluation globale des trois systèmes n'est faite ici qu'à titre d'exercice. Je ne prétend certainement pas qu'elle est exempte de tout reproche. La définition d'une méthode d'évaluation

correcte et objective pouvant à elle seule faire l'objet d'un mémoire et étant assez étrangère au sujet qui nous occupe, je n'approfondirai pas la question.

Dans tous les cas, quelle que soit la méthode, la recherche de l'objectivité passe par l'évaluation par plusieurs personnes d'horizons divers (cette multi-évaluation n'a pas été faite ici).

Bibliographie

- [AXI] Les cartes à mémoire, Axis, Ecomédia, 1989
- [BEA] La transmission des résultats d'analyses médicales en médecine extra-hospitalière - Une ouverture à l'automatisation du Dossier Médical de médecine générale, Beauloye M. et Ramaekers J., Louvain Med 109: 413-424, 1990
- [BE2] Lettre du Docteur M. Beauloye à l'Ordre des Médecins du 21 novembre 1990
- [BOU] Recommandations relatives à la transmission de documents se rapportant aux analyses de biologie médicales, Bourse R., Feuillet de biologie vol 26 n°145: 21-24, 1985
- [BO2] Réflexions sur la télématique et le laboratoire de biologie clinique, Bourse R., feuillets de biologie vol XXV n°139 p23 à 27, 1984
- [BON] Le secret professionnel et les professions de santé, Bonneau J., Vie sociale n°9-10 p417 à 426, septembre-octobre 1989
- [CAR] "Do-it-yourself" cryptography, Carroll J.M., Computers & Security volume 9 number 7 p613-619, novembre 1990
- [CNI] La santé et l'aide sociale, Rapport de la CNIL, Dix ans d'informatique et libertés Chap. 10 193 Economica Paris, 1988
- [CO1] Biologie Clinique et transmission des résultats - Avis du Conseil National, -, Bul. Conseil O.M. 34: 40, 1986
- [CO2] Biologie Clinique et transmission des résultats - Avis du Conseil National, -, Bul. Conseil O.M. 38: 16, 1987
- [CO3] Biologie Clinique et transmission des résultats - Avis du Conseil National, -, Bul. Conseil O.M. 45: 20-21, 1989
- [DAV] Security for computer networks: an introduction to data security in teleprocessing and electronic funds transfer, Davies, D.W. and Price W.L., Wiley Chichester, 1984
- [DEH] Séance inaugurale du 7e congrès international belgo-néerlandais d'informatique médicale Anvers, Dehaene J.L., -, mars 1987
- [DEM] Readings in Medical Infomatics, De Moor G., MIM Medical Informatics Conference Antwerp Belgium, 15 septembre 89
- [DEN] Banques de données: quelle protection juridique ? Denis S., Pouillet Y., Thunis X., Cahiers du CRID n°2 Facultés Universitaires Notre-Dame de la Paix de Namur Story-Scientia, 1988

- [FON] Systèmes de télécommunications: Bases de transmission, Fontolliet P.-G., Dunod, 1983
- [FRI] Contribution à la sécurisation de la transmission télé-informatique de résultats d'analyses biomédicales entre le laboratoire d'analyses et le médecin prescripteur, Frisque P., FUNDP Institut d'Informatique, 1989
- [GAN] La carte à mémoire, Roger Ganne et Brigitte Salomoni, Eyrolles, 1990
- [GRA] Informatique, délinquance et vie privée: les nouveaux dangers du traitement informatique des données médicales, Grandjean I., UCL Ecole de Criminologie, 1985
- [GR1] Le Dossier du malade, Gremy F., Informatique Médicale ch.8: 164-191 Flammarion Médecine-Sciences Paris, 1987
- [GR2] Systèmes d'information dans le cabinet du praticien "libéral", Gremy F., Informatique Médicale ch.15: 328-362 Flammarion Médecine-Sciences Paris, 1987
- [GR3] Protection des données médicales nominatives, Gremy F., Informatique Médicale ch.19: 421-458 Flammarion Médecine-Sciences Paris, 1987
- [GUE] Les cartes à microcircuit: théorie et applications, Guez F., Robert C. et Lauret A., Masson, 1988
- [HUB] Application de la cryptographie à la sécurisation d'un réseau informatique à l'aide d'un processeur de sécurité, Hubin J., FUNDP Institut d'Informatique, 1990
- [JAM] Information et informatisation en médecine générale - Journées d'initiation à l'informatique au cabinet médical, Jamouille M., Institut d'informatique Archimède Namur, 1987
- [JAN] La sécurité informatique, Jan Ch. et Sabatier G., Eyrolles, 1989
- [ITS] Information Technology Security Evaluation Criteria (ITSEC), Communautés européennes, -, 1990
- [MON] Vers une nouvelle réglementation des télécommunications, Monville C., Pouillet Y., Van Bastelaer Ph., Amory B., de Meester J.C., Defraigne Ph., Janfils Ch., Queck R., Cahiers du CRID n°4 Facultés Universitaires Notre-Dame de la Paix de Namur Story-Scienta, 1990
- [PO1] Sécurité informatique et données médicales, Pouillet E., Louvain Med 105: 531-537, 1986
- [VUL] La CNIL et le secteur de la santé, Vulliet-Tavernier S., Vie sociale n°9-10 p435 à 444, septembre-octobre 1989

- [WAR] Confidentialité du dossier médical informatisé - Communication au Groupement des Gynécologues et Obstétriciens de langue française, Warrant F., -, 1989
- [WA2] Recherche épidémiologique et protection des données médicales nominatives: état de la question en Belgique, Warrant F., CRID, septembre 89

Liste des figures

fig 1: Notations pour chiffrement et déchiffrement	31
fig 2: Le chiffrement de Vernam	36
fig 3: Schéma de principe d'une écoute passive	38
fig 4: Schéma de principe d'une écoute active	39
fig 5	41
fig 6: Exemple de chiffrement produit	43
fig 7: Structure logique du DES	44
fig 8: Chiffrement par chaînage de blocs	46
fig 9: Erreur d'un seul bit (méthode CBC)	48
fig 10: Principe du chiffrement à clé publique	51
fig 11: Identification du porteur de la carte	73
fig 12: Authentification du porteur de la carte	74
fig 13	80
fig 14: Droit de regard de l'autorité	103
fig 15: Schéma du système TRASEC	107
fig 16: Terminal TRASEC	108

Liste des tableaux

tableau 1: Comparaison des modes de transmission	11
tableau 2: Distribution de clés par fonction exponentielle . .	49
tableau 3: Table des puissances et exponentielles modulo 11 . .	50
tableau 4: Carte à microprocesseur: organisation de la mémoire	71
tableau 5: Zones de la carte à microprocesseur	72