*E.N.S.S.I.B.*
Ecole Nationale Supérieure
des Sciences de l'Information
et des Bibliothèques

U.C.B.L.
Université
Claude Bernard
LYON I

**DESS en INFORMATIQUE DOCUMENTAIRE**

**Rapport de recherche bibliographique**

# *Sécurité sur Internet*
# ...
# *Techniques de chiffrement, Domaines d'utilisation et Législation en France*

**Denis Philippon**

Sous la direction de

**M. Jean-Pierre Lardy**

**U.R.F.I.S.T. de LYON**



**Année 1996-1997**

*E.N.S.S.I.B.*
Ecole Nationale Supérieure
des Sciences de l'Information
et des Bibliothèques

U.C.B.L.
Université
Claude Bernard
LYON I

**DESS en INFORMATIQUE DOCUMENTAIRE**

**Rapport de recherche bibliographique**

# *Sécurité sur Internet*
# ...
# *Techniques de chiffrement, Domaines d'utilisation et Législation en France*

**Denis Philippon**



Sous la direction de

**M. Jean-Pierre Lardy**

**U.R.F.I.S.T. de LYON**

**Année 1996-1997**

# *Sécurité sur Internet*
# ...
# *Techniques de chiffrement, Domaines d'utilisation et Législation en France*

**Denis Philippon**

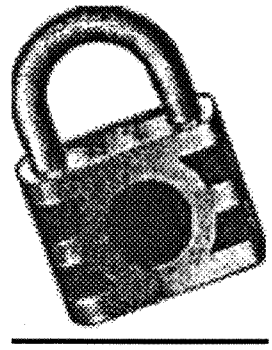
Résumé : L'augmentation croissante des besoins de sécurité sur l'Internet entraîne l'utilisation de techniques de chiffrement. En effet, certains domaines ne peuvent plus se permettre d'effectuer des transactions « peu sûres ». Pourtant, la législation française est très restrictive actuellement quant à son utilisation. Qu'en sera-t-il demain ?.

Descripteurs : Cryptologie / Cryptographie / Chiffrement / Internet / Réseau / Sécurité / Législation

Abstract : The increasing growth of security needs in the Internet are leading to the use of encoding technics. In fact, in some fields it is not any more possible to take the liberty of doing « not very secured » transactions. Nevertheless, the French legislation today is very restrective as for its use. But what has the future in store for us ?

Keywords : Cryptology / Cryptography / Internet / Network / Security / Legislation

# SOMMAIRE



# 1. Préambule

L'objet de cette recherche est de déterminer les techniques de chiffrement logiciel (par opposition aux techniques matérielles) utilisées sur l'Internet. Les différents domaines d'application de ces techniques seront ensuite abordés. Enfin, un point sur la législation en France, en matière de chiffrement, sera effectué.

# 2. Recherche

## *2.1 Les CD-ROM*

### 2.1.1 BNF

Il s'agit d'un CD-ROM de la Bibliothèque Nationale de France (B.N.F.). Elle possède 800.000 notices bibliographiques d'ouvrages entrés par dépôt légal depuis 1970. Cela concerne des ouvrages imprimés et des publications officielles de grands organismes nationaux.

| Champ interrogé | Descripteur | Résultats bruts | Résultats pertinents | Taux de pertinence |
|---|---|---|---|---|
| Mot notice (mc) | chiffrement | 20 | 8 | 40 % |
| Mot notice (mc) | cryptographie | 23 | 9 | 39 % |
| Mot notice (mc) | cryptologie | 20 | 9 | 45 % |
| Résultat global | | 26 | 11 | 42 % |

La pertinence des ouvrages a été déterminée en fonction de leurs titres ou de leur apparition lors de recherches autres.

### 2.1.2 BN OPALE

Il s'agit d'un CD-ROM établit par Bibliothèque Nationale. Cela concerne des notices d'autorités. Elle possède 550.000 notices de personnes physiques et collectivités. Il s'agit de titre uniforme et matière (RAMEAU) d'ouvrages catalogués.


| Champ interrogé | Descripteur | Résultats bruts | Résultats pertinents | Taux de pertinence |
|---|---|---|---|---|
| Mot clé dans tout le fichier (tt) | crypto$ | 31 | 17 | 55 % |
| Mot clé dans tout le fichier (tt) | chiffrement | 2 | 2 | 100 % |
| Résultat global | | 32 | 18 | 56 % |

La pertinence de ces ouvrages a put être déterminée grâce à la présence d'un résumé lors de l'interrogation. Il faut remarquer qu'il ne m'était pas possible de traduire certains résumés (russe, hongrois).

### 2.1.3 LISA +

Library and Information Science Abstracts Plus (LISA +).
Il s'agit d'un CD-ROM établit par la Library Association et par l'ASLIB (deux associations professionnelles anglaises). Cela concerne tous types de documents. C'est une base spécialisée en sciences de l'information et bibliothéconomie.


| Champ interrogé | Descripteur | Résultats bruts | Résultats pertinents | Taux de pertinence |
|---|---|---|---|---|
| Résumé (ab) | crypto$ | 23 | 11 | 48 % |

Même remarque que pour le CD-ROM « BN OPALE ».

### 2.1.4 CD-ROM DOC-THESES

Il s'agit d'un CD-ROM sur toutes les thèses de doctorat soutenues dans les universités françaises depuis 1972 (lettres, sciences humaines et sociales, sciences). Il inclut depuis 1983 les thèses de santé.
CD-ROM édité par le Ministère chargé de l'enseignement supérieur (ABES).


| Champ interrogé | Descripteur | Résultats bruts | Résultats pertinents | Taux de pertinence |
|---|---|---|---|---|
| Mot-clé | cryptographie | 2 | 0 | 0 % |

Les deux thèses ne correspondent pas au sujet traité. En effet, la première datant de 1993 et réalisée par Antoine Joux concernait l'utilisation de la cryptographie afin de ´ réduire les réseaux ». La deuxième réalisée par H. Richy en 1978 ne peut plus être considérée comme pertinente puisque l'avancée technologique dans ce domaine a beaucoup évoluée.

## *2.2 Dialog*

Bases de données interrogées :

| Numéro de la base (file) sous Dialog | Nom de la base langue(s) utilisée(s) « Producteur » | Sujets abordés | Période de référence des documents |
|---|---|---|---|
| **144** | **Pascal**,<br>Anglais et français,<br>INIST / CNRS | Sciences multidisciplinaires | De 1973 à nos jours |
| **2** | **INSPEC**,<br>Anglais,<br>Institution of Electrical Engineers | Physique, électronique, électricité, ordinateurs et technologies de l'information | De 1969 à nos jours |
| **275** | **Computer Database**,<br>Anglais,<br>Info Access Co | Matériel, logiciels, télécommunications et électroniques | De 1983 à nos jour |
| **674** | **Computer News Fulltext**,<br>Anglais,<br>IDG Communications | Ordinateurs et réseaux informatiques | De 1974 à nos jour |
| **8** | **Ei Compendex Plus**,<br>Anglais,<br>Engineering Info. Inc. | Ingénierie | De 1970 à nos jours |

La sélection, sous Dialog, de ces bases s'effectue en tapant la commande :

**B 144,2,275,674,233,8**

Abréviations utilisées :

- C.D. : Computer Database,
- C.N.F. : Computer News Fulltext,
- Cx : Compendex,
- DE : Descripteur,
- PY : Publication Year,
- RD : Elimination des doublons entre les bases de données.

Questions posées et résultats obtenus :

| N° question | Question | Pascal | Inspec | C.D. | C.N.F. | Cx | Total |
|---|---|---|---|---|---|---|---|
| S1 | S CRYPTOGRAPHY/DE (*) | 1.127 | 5.375 | 281 | 137 | 2.234 | **9.154** |
| S2 | S INTERNET/DE (*) | 1.165 | 3.676 | 12.473 | 9.812 | 1.654 | **32.718** |
| | OR INTRANET/DE | 6 | 0 | 633 | 905 | 26 | **1.572** |
| S3 | S SECURITY / DE (*) | 445 | 12.406 | 12.330 | 6.468 | 5.366 | **39.735** |
| S4 | S1 AND S2 AND S3 | 34 | 114 | 20 | 105 | 387 | **660** |
| S5 | S4/PY=1995:1996 | 22 | 26 | 1 | 61 | 183 | **293** |
| S6 | RD S6 | | | | | | **274** |

(*) Descripteur (DE) non utilisé pour C.N.F. et Compendex.

Les 100 premières références ont été extraites de la sélection finale. En utilisant le résumé des documents, la pertinence s'élève à 93 %. En effet, certains documents concernent la sécurité appliquée aux appareils portables, d'autres concernaient la circulation des images (animées ou fixes) sur l'Internet ...

## *2.3 Les bibliothèques*

### 2.3.1 La Bibliothèque de l'ENSSIB

Interrogation par mots du sujet sur les monographies.

| Champ interrogé | Descripteur(s) | Résultats bruts | Résultats pertinents | Taux de pertinence |
|---|---|---|---|---|
| Mot du sujet | Cryptographie | 4 | 3 | 75 % |
| Mots du sujet | Commerce ET réseau | 2 | 1 | 50 % |
| Mots du sujet | Législation ET réseau | 4 | 0 | 0 % |

Les trois-quarts des documents concernant la cryptographie sont pertinents (deux documents concernent une édition et sa réédition augmentée). Un document concerne un stage d'étudiant au DESSID. Concernant le commerce et les réseaux, un seul document de Bill Gates (La route du futur) aborde le sujet car l'autre concerne la mise en réseau de CD-ROM. Enfin, concernant la législation et le réseau, aucun document ne concernait le sujet traité.

### 2.3.2 DOC'INSA

Interrogation de la base INSADOC grâce à Internet.

Interrogation par mot-clé sur les monographies.

| Champ interrogé | Descripteurs | Résultats bruts | Résultats pertinents | Taux de pertinence |
|---|---|---|---|---|
| Mot clé | (cryptolog* or cryptogr* or chiffrement*) and Internet | 4 | 4 | 100 % |

Tous les documents récupérés grâce à cette interrogation s'avéraient pertinents. De plus, ces documents étaient tous récents (de 1995 à 1996).

### 2.3.3 La Bibliothèque de la Part-Dieu

Interrogation par descripteur sur les monographies (catalogue GEAC)

| Champ interrogé | Descritpeur | Résultats bruts | Résultats pertinents | Taux de pertinence |
|---|---|---|---|---|
| descripteur | Chiffrement | 4 | 4 | 100 % |
| descripteur | Cryptographie | 5 | 4 | 80 % |

La majorité des documents sont pertinents, quoique peu récents pour certains. Un seul roman a été référencé avec le mot-clé « Cryptographie ». Il faut remarquer qu'un document référencé avec un descripteur ne pouvait être retrouvé à l'aide de l'autre descripteur.

### 2.3.4 Médiathèque de Villeurbanne (cours Emile Zola)

Interrogation par descripteur sur les monographies (logiciel OPSYS - par minitel)

| Champ interrogé | Descripteur | Résultats bruts | Résultats pertinents | Taux de pertinence | Commentaires |
|---|---|---|---|---|---|
| descripteur | Réseau et télécommunication | 6 | 3 | 50 % | Monographies |
| descripteur | Internet / législation | 2 | 1 | 50 % | Périodiques |
| descripteur | Commerce / Internet | 1 | 1 | 100 % | Périodique |

Concernant les monographies, trois documents abordaient les réseaux informatiques et ses différentes couches (et donc les cryptage des messages). Concernant Internet et la législation, un article ne pouvait pas être considéré comme pertinent puisqu'il abordait les droits d'auteur des créations numériques.

Comme à la Bibliothèque de la Part-Dieu, un document référencé avec un descripteur ne pouvait être retrouvé à l'aide d'un autre descripteur.

## *2.4 Internet*

### 2.4.1 Les FAQs (Frequently Asked Questions)

Université LYON I : **ftp.univ-lyon1.fr/faq/by_name**
Mot-clé : ***crypto***

Université de l'Ohio : **http://www.cis.ohio-state.edu/htbin/search-usenet.faqs**
(Etats-Unis, C.I.S.) Mot-clé : ***crypto***

### 2.4.2 Les moteurs de recherche

| Moteur | Question | Réponses |
|---|---|---|
| ALTAVISTA | (cryptography or cryptology) and (Internet or intranet) | 10.000 réponses |
| ALTAVISTA | (cryptographie or cryptologie or chiffrement) and (Internet or intranet) | 800 réponses |
| YAHOO | (cryptography or cryptology) and (Internet or intranet) | 5030 réponses |
| INFOSEEK | cryptography and Internet | 114 réponses |
| LYCOS | (cryptography or cryptology) and (Internet or intranet) | 7.652 réponses |
| LYCOS | (cryptographie or cryptologie or chiffrement) and (Internet or intranet) | 43.482 réponses |

### 2.4.3 Les news

Certaines informations ont étés retrouvées en consultant une serveur de « news ».

**http://xp6.dejanews.com**

**Question :** ( chiffrement OU cryptographie ) ET ( internet OR intranet )

**Résultats :**

| | |
|---|---|
| (1) chiffrement : | 145 réponses |
| (2) cryptographie : | 114 réponses |
| (3) internet : | 1.880.229 réponses |
| (4) intranet : | 18.300 réponses |
| ( (1) OU (2) ) ET ( (3) OU (4) ) : | 63 réponses |

La volabilité et le non-contrôle de ces messages, inhérents à la fonction des news rend difficile l'établissement d'un taux de pertinence des différents messages se trouvant sur ce serveur.
Nous nous contentons donc de citer ce serveur ainsi que les mots-clés permettant d'accéder à une liste abordant le sujet. Nous vous invitons tout de même à les consulter car leur « fraîcheur » est par ailleurs des plus intéressante. Nous citerons par exemple les indiscrétions sur le futur décret de réglementation de la cryptologie sur Internet ainsi que les derniers algorithmes « crackés ».

## *2.5 Le coût de la recherche*

### 2.5.1 Temps

| | |
|---|---|
| CD-ROM | 3,50 h. |
| Internet | 38,00 h. |
| Dialog | 1,50 h. |
| Bibliothèques | 8,00 h. |
| Lecture | 47,00 h. |

### 2.5.2 Coût financier

Celui-ci n'est chiffrable que sur l'interrogation des bases de données sur Dialog. En effet, l'interrogation des bases de données sur CD-ROM est gratuite ainsi que l'accès à Internet (à l'université bien entendu).

Dialog : $16.08

# 3. Synthèse

## *3.1 Introduction*

Le moyen de communication mondial que représente le réseau Internet et l'augmentation toujours croissante de ses « abonnés » entraîne automatiquement un besoin grandissant de sécurité des informations qui y transitent. En effet, tout message circulant sur le réseau est en clair. Cela signifie que tout personne peut intercepter ce dernier et utiliser à des fins « douteuses » les informations.

Ceci entraîne un besoin grandissant d'utilisation des techniques de chiffrement (algorithme). Nous allons donc présenter ces techniques avant d'aborder les domaines concernés par cette sécurité et nous finirons par la législation en vigueur (et à venir) en France.

## *3.2 Techniques de chiffrement*

Plusieurs techniques de chiffrement sont apparues. Celles-ci utilisent des algorithmes assurant un niveau de sécurité différent mais toujours très correct. Nous allons donc présenter les algorithmes utilisés puis les « logiciels » les mettant en application.

### 3.2.1 Les algorithmes

Un des précurseurs fut Jules César [1]. Il adoptait, pour correspondre avec Cicéron une technique de décalage des lettres de son message. En effet, le « a » devenait « d », le « b » un « e » etc.

Plus récemment, une méthode consistait à additionner le poids des lettres (ordre dans l'alphabet) avec le poids des lettres d'une clé. On effectuait sur cette addition un modulo 26 et on obtenait le message codé.

| | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ex : | Message original : | INTERNET A SECURISER | | | | | | | | | | | | | | | |
| | Message à traiter : | I | N | T | E | R | N | E | T | A | S | E | C | U | R | I | S | E | R |
| | | 9 | 14 | 20 | 5 | 18 | 14 | 5 | 20 | 1 | 19 | 5 | 3 | 21 | 18 | 9 | 19 | 5 | 18 |
| | Clé : | D | E | S | S | I | D | D | E | S | S | I | D | D | E | S | S | I | D |
| | | 4 | 5 | 19 | 19 | 9 | 4 | 4 | 5 | 19 | 19 | 9 | 4 | 4 | 5 | 19 | 19 | 9 | 4 |
| | Message chiffré : | M | S | M | X | A | R | I | Y | T | L | N | G | Y | W | B | L | N | V |
| | | 13 | 19 | 13 | 24 | 1 | 18 | 9 | 25 | 20 | 12 | 14 | 7 | 25 | 23 | 2 | 12 | 14 | 22 |
| | Message envoyé : | MSMXARIY T LNGYWBLNV | | | | | | | | | | | | | | | |

[1] **Oilvier Andrieu, Denis Lafont** / *INTERNET et l'ENTREPRISE* - EYROLLES - sept. 1995, 395 p., p. 248-253, ISBN : 2-212-08906-6

En connaissant la clé, on effectuera donc le chemin inverse pour déchiffrer le message.

De nos jours, il existe deux classes d'algorithmes à base de clé : Les algorithmes dits « symétriques » (ou à clé secrète) et les algorithmes « asymétriques » (ou à clé publique). Les algorithmes symétriques utilisent la même clé pour chiffrer et déchiffrer un message (ou la clé de décryptage est facilement dérivable de la clé de cryptage). A l'inverse, les algorithmes asymétriques utilisent des clés de chiffrement et déchiffrement différentes et ne pouvant pas être déduites l'une par rapport à l'autre.

L'algorithme DES

L'algorithme DES (Data Encryption Standard) date de 1975 et a été créé par IBM. Il a pour avantage sa grande rapidité de chiffrement et de déchiffrement. De plus, il est très court à programmer et possible à implanter sur des cartes électroniques (puces ...). Les brevets de codage de DES appartiennent à IBM mais ils ont été cédés à l'état américain pour une utilisation libre. Il est donc libre de droits, c'est la raison pour laquelle il est très largement répandu.

Cet algorithme utilise une clé de chiffrement identique à la clé de déchiffrement. L'émetteur et le destinataire doivent donc connaître cette clé préalablement à l'envoi/réception du message. Implicitement, la communication de cette clé doit être effectuée en dehors du réseau. Ce processus est appelé « symétrique » et à « clé secrète ».

Principe de fonctionnement [2] :

1°) Découpage du texte clair en blocs de 64 bits séparés eux-mêmes en blocs de 32 bits.

2°) On mélange et on répète chaque bloc de 32 bits afin d'obtenir 48 bits.

3°) On effectue un « OU exclusif » de chaque bloc de 48 bits avec chaque bit (16) d'une clé calculée à partir de la clé d'origine sur 8 octets (64 bits).

4°) On découpe les 48 bits obtenus en 8 blocs de 6 bits. Chacun de ces nouveaux blocs font référence à une table de substitution. On substitue alors un bloc trouvé dans la table au bloc d'origine. Après ces manipulations successives, on obtient un nouveau bloc de 32 bits.

5°) On effectue une nouvelle permutation de ce bloc de 32 bits.

6°) On effectue alors un « XOR » entre ce bloc de 32 bits et le premier bloc de 32 bits créé lors de la séparation des blocs de 64 bits.

On peut remarquer qu'avec l'explosion d'Internet, il est apparut le triple-DES (clés de trois fois 56 bits). Ce dernier permet une quasi-invulnérabilité de chiffrement.

---

[2] **Xavier Marsault**, *Compression et cryptage des données multimédias* - 2è édition revue et augmentée, Traité des Nouvelles Tech, série Informatique, Paris, Hermès - sept. 1995, p. 141-147, 152-155 - ISBN : 2-86601-482-0.

L'algorithme RSA

L'algorithme R.S.A (du nom des inventeurs Rivest, Shamir et Adleman) date de 1977.

C'est un système de chiffrement à clé publique. Il repose sur un système à deux clés liées. L'une est publique et connue de tous alors que l'autre est secrète et connue seulement de l'émetteur et du destinataire.

*Remarque* : L'algorithme R.S.A. est breveté aux Etats-Unis mais ce brevet n'est pas valable en dehors. Il est donc utilisable librement (hors législation sur la cryptographie) en dehors des U.S.A.

Principe de fonctionnement :

1°) On choisit deux très grands nombres premiers que l'on multiplie.

2°) Ce nouvel entier va moduler (de modulo) le message à coder.

3°) On décompose le message en blocs. Sur chacun de ces blocs on calcule le modulo, après avoir appliqué un exposant secret, grâce à l'entier déterminé précédemment.

La supériorité (en vitesse) de l'algorithme DES sur RSA a été démontré. En effet, Xavier Marsault cite un rapport de 100 fois plus rapide en chiffrement logiciel et de 1.000 à 10.000 fois lorsqu'il est câblé. La survie de RSA dépend donc de la mise au point d'un algorithme permettant d'effectuer une factorisation rapide pour décoder les messages codés.

Il faut remarquer qu'il existe un algorithme dérivé de RSA permettant de chiffrer le courrier électronique : Il s'appelle RSA-MD2.

### 3.2.2 Les logiciels

Le programme PGP

Le programme PGP (Pretty Good Privacy) de Phil Zimmerman (USA) permet de chiffrer et déchiffrer des messages à l'aide de l'algorithme RSA. Une de ses fonctions est aussi de permettre de conserver des fichiers de clés de chiffrement. PGP est disponible sur Internet mais totalement interdit par la loi française en vigueur (voir le chapitre sur la législation). Il faut aussi remarquer que l'auteur a fait l'objet de très longues poursuites judiciaires par l'Etat américain.

Le système PEM

Le système PEM (Privacy-Enhanced Mail) permet de protéger l'intégrité et la confidentialité du courrier électronique.

Le logiciel RIPEM

Le logiciel RIPEM (Riordan's Internet Privacy-Enhanced Mail) permet d'assurer la confidentialité du courrier électronique, l'authentification de son expéditeur, la vérification de son intégrité et la non répudiation. Il s'appuie sur l'algorithme RSA.

*Le code de Mark Riordan fait partie du domaine public.*

La technologie Clipper (USA, 1993) [3]

C'est une technologie américaine (à l'initiative de Bill Clinton) qui oblige que tout appareil doit posséder deux clés. L'une pour l'utilisateur et l'autre pour le gouvernement afin de pouvoir « tracer » les messages codés si le besoin s'en faisait ressentir. Le dépôt de cette deuxième clé est effectué dans des agences mandatées par le gouvernement. La confidentialité du message que vous envoyez n'est donc plus absolue car un tiers peut, s'il le désire, relire vos messages.

Le protocole S.S.L.

Le protocole S.S.L. (Secure Sockets Layer) de Netscape est un protocole de communication qui est indépendant des autres protocoles. Les autres protocoles existants tels que ftp, telnet, http ... peuvent l'utiliser pour chiffrer à loisir les messages transmis et reçus. Ce protocole s'appuie sur l'algorithme RSA. Ce protocole est dorénavant intégré au navigateur Netscape. SSL ne fonctionne que dans le cadre d'échanges entre navigateurs.

Remarque : Il est important de signaler que le protocole SSL a déjà été « cracké ».

1.Un autre protocole proche de SSL est apparut grâce à RSA épaulé avec un grand nombre d'acteurs du commerce électronique (America Online, Compuserve, IBM ...). Ce protocole est appelé S-HTTP (Secure HTTP). D'autres protocoles concurrents émergent aussi tels que Jepi (Commerce Net) et SET - Secure Electronic Transactions - développé par Mastercard, Visa, IBM, Netscape ...

S.S.H.

S.S.H. (Secure Shell) est une version sécurisée des programmes de connexion UNIX (rlogin, rsh et rcp). Leurs « doubles » sécurisés (slogin, ssh, scp) fonctionnent à l'identique tout en effectuant automatiquement et de façon transparente de l'authentification et du chiffrement.

Le protocole SHTTP

Le protocole SHTTP (Secure HTTP) permet de sécuriser les transactions entre client et serveur HTTP dans le cadre d'applications commerciales. Ce protocole utilise PEM, PGP ou PKCS-7.

[3] **John Vacca** (1996), *Sécurité sur Internet - Secrets*, Sybex, 938 p., ISBN : 2-7361-2135-X

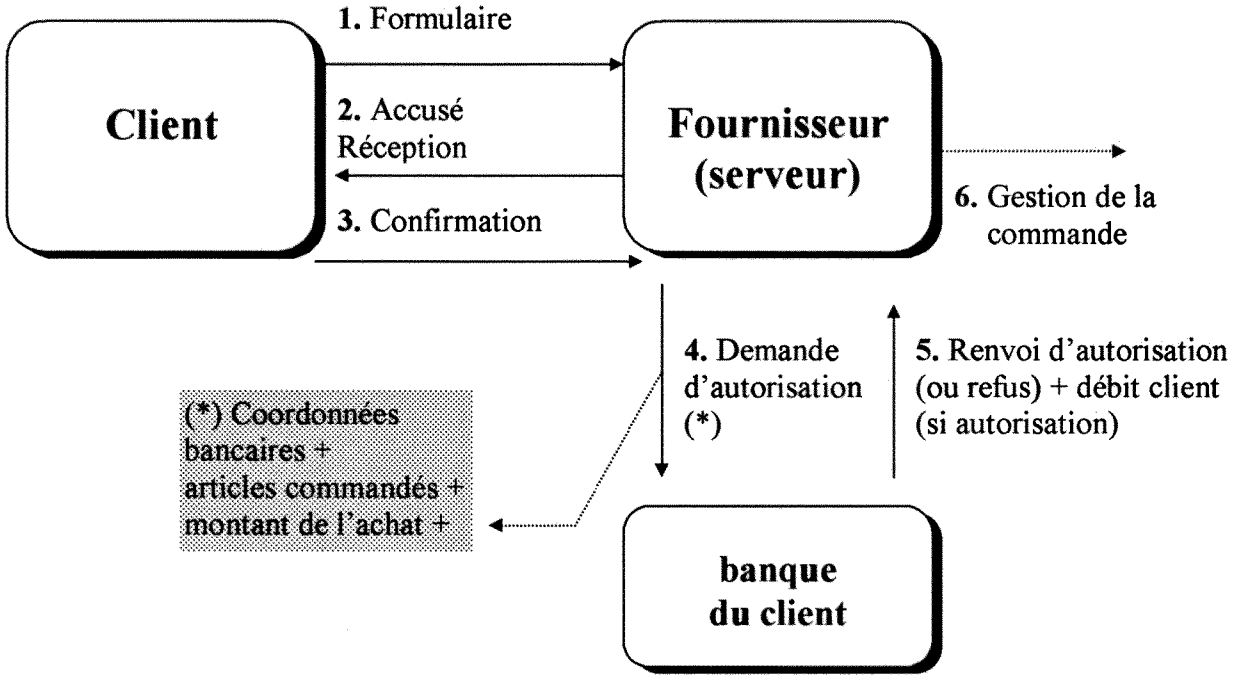
### *3.3 Domaines d'utilisation*

Le besoin de « sécurisation » des messages transmis devient fondamental dès que l'on aborde le courrier ou le commerce électronique.

En effet, l'Expansion du 19 décembre 1996 [4] cite une estimation faite par le vice-président du cabinet d'audit Booz, Allen & Hamilton comme quoi 20 % des dépenses des ménages transiteront par Internet. Cette estimation non vérifiable permet tout de même de penser que le besoin de sécurisation des informations commerciales va suivre une courbe exponentielle dans les années à venir.

Pour respecter la législation française (cf chapitre sur la législation), un certain nombre de « cyberbanques » ont été autorisées par l'Etat à utiliser le chiffrement des messages afin d'effectuer des opérations financières sécurisées sur l'Internet.

Principe de fonctionnement :



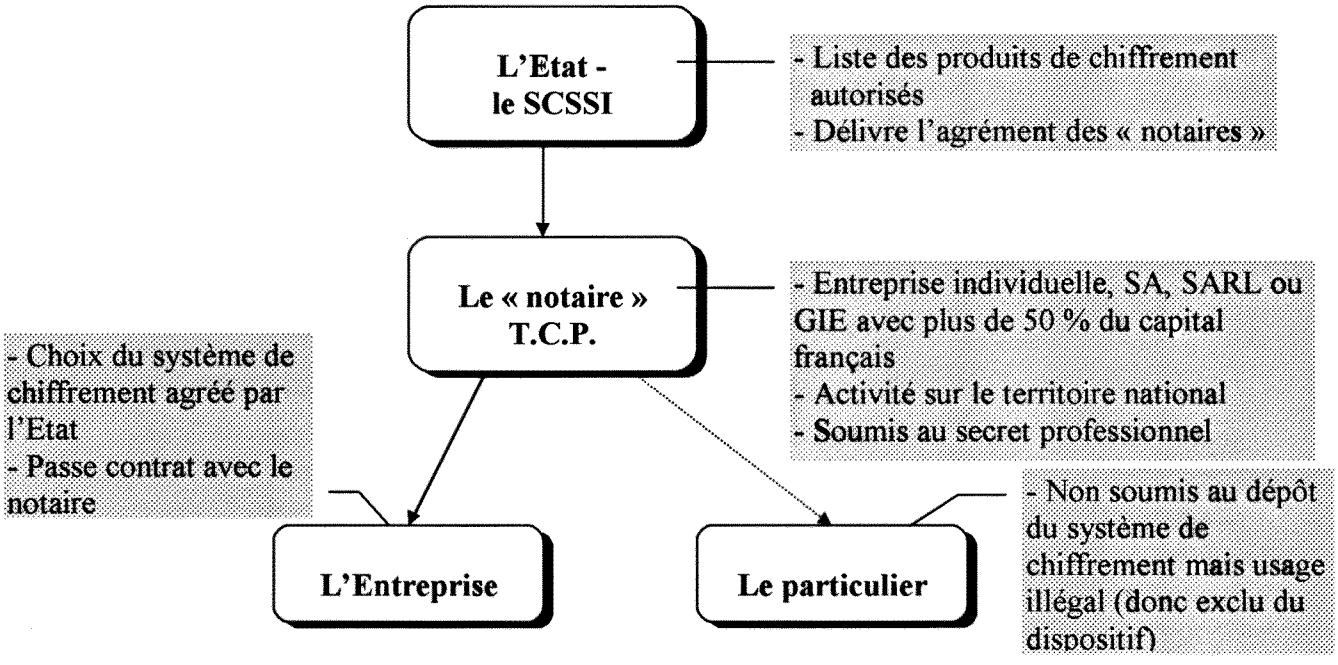

[4] **Gilles Pouzin, Thierry Fabre, Gilles Fontaine** (déc. 1996), *Entrez dans l'âge du cybercommerce*, L'Expansion N° 539, 20 F., p.66-77

### *3.4 La législation française*

La loi N° 96-659 du 26 juillet 1996 [5](Journal Officiel du 27 juillet 1996) de réglementation des télécommunications stipule que toute personne ou organisme voulant chiffrer un message doit préalablement demander une autorisation préalable aux services du premier Ministre. Un projet de loi (voir annexe) envisage de confier cette tâche à des tiers de confiance (cf schéma ci-après) indépendants de l'Etat qui seront agréés par le Premier ministre. En effet, tout acteur voulant crypter des informations devra remettre les clés de son programme de cryptage préalablement à son utilisation. Ses codes seront secrètement gardés par le tiers de confiance, hormis dans le cadre de commissions rogatoires policières.

La personnalité juridique de ces tiers de confiance n'est par encore déterminée. Il faut tout de même se rappeler que ne seront soumis à cette législation que les entreprises et personnes dont le pays d'établissement est la France. Il faut donc constater qu'un vide juridique existera tant que des dispositions internationales concernant le chiffrement sur l'Internet ne seront pas prises.

Organisation « à venir » [6] des Tierces Parties de Confiance (TCP)
*Voir projet de décret en annexe.*




**SCSSI** : Service Central pour la Sécurité des Systèmes d'Information (il dépend du SGDN, bras défense de Matignon).

---

[5] **Lois et décrets** / *loi n° 96-659 de réglementation des télécommunications* - Journal Officiel (JO), n° 174 - 27 juill. 96, p. 11384-11400 - ISSN : 0373-0425.

[6] Crypto - *Avant-première sur la réglementation* - Planète Internet, n° 15 - Janv. 1997, p. 21, 30 F. - ISSN : 1267-3331. Voir aussi sur Internet : http://www.planete-internet.com/crypto/decret (futur décret)

### *3.5 Conclusion*

On peut donc dire que l'utilisation des diverses techniques de chiffrement va aller crescendo. L'invulnérabilité des algorithmes va encore se renforcer face aux multiples « pirates » (hackers en anglais).

En effet, les besoins sont énormes et l'attente du public est réelle. Il faut donc impérativement que les législations s'adaptent à cette nouvelle technologie et à ses conséquences économiques. Les enjeux mondiaux que représente l'Internet doivent inciter à une harmonisation de la législation.

## 4. Glossaire [7]

### *Algorithme cryptologique*

Un algorithme cryptologique est un procédé permettant, à l'aide d'une clé de chiffrer et de déchiffrer des messages ou des documents.

### *Authentification*

Authentifier, c'est s'assurer que l'émetteur du message est bien la personne qui l'a émit.

Authentifier un utilisateur, c'est s'assurer qu'il est bien celui qu'il prétend être.
Authentifier un document, c'est s'assurer qu'il est bien tel que son auteur l'a écrit.

### *Chiffrer*

Chiffrer, c'est transformer un texte clair en texte chiffré. L'opération ou son résultat s'appelle un « chiffrement ». (Les verbes « crypter » et « encrypter » sont des anglicismes tolérés).

### *Clé*

Les bons algorithmes cryptologiques ont besoin d'une clé pour chiffrer (la clé de chiffrement) et pour déchiffrer (la clé de déchiffrement). Parfois, c'est la même.

### *Clé publique, clé privée*

Quand les clés de chiffrement et de déchiffrement ne peuvent pas se déduire l'une de l'autre, on peut sans dommage publier l'une des deux, qui devient une clé publique. L'autre est une clé privée. Si c'est la clé de chiffrement qui est publique, tout le monde peut chiffrer un message que seul celui qui connaît la clé privée correspondante peut déchiffrer. C'est un moyen d'assurer la confidentialité. Si, au contraire, c'est la clé de déchiffrement qui est publique, seul celui qui connaît la clé privée peut chiffrer un message que n'importe qui pourra déchiffrer. Evidemment, la confidentialité ne sera pas assurée ; en revanche, on est sûr que l'auteur du message connaît la clé privée. C'est un moyen de prouver son identité, c'est-à-dire de l'authentifier.

### *Clé secrète*

Quand les clés de chiffrement et de déchiffrement ne peuvent se déduire l'une de l'autre, et à plus forte raison quand c'est la même, on ne peut pas les publier. On parle alors de clés secrètes.

---

[7] voir le site Internet http://www.planete.net/~jbaagoe/Confidentiel/glossaire.html

***Confidentialité***

Assurer la confidentialité d'un document ou d'un message, c'est s'assurer que seules les personnes autorisées à le lire peuvent le faire.

***Contrôle d'accès***

Le contrôle d'accès détermine, après l'avoir authentifié, quelles sont les autorisations (de lecture, d'écriture, etc.) d'un utilisateur. Si l'authentification échoue, la connexion n'est pas établie : c'est un cas extrême de refus de services.

***Cryptologie, cryptographie, cryptanalyse***

La cryptologie est l'ensemble des techniques visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse (Loi no 90-1170 sur la réglementation des télécommunications, J.O. du 30/12/94). On distingue parfois entre la cryptographie, qui est l'art de concevoir de telles techniques, et la cryptanalyse, qui est l'art de les briser. Ainsi, la cryptologie serait un sur-ensemble de la cryptographie, puisqu'elle comprendrait la cryptanalyse en plus. Mais cette distinction reste assez théorique : les deux termes « cryptologie » et « cryptographie » sont en fait le plus souvent utilisés comme synonymes.

***Déchiffrer, décrypter***

Déchiffrer, c'est traduire en clair en connaissant la clé. C'est donc le destinataire légitime du message, Décrypter, c'est traduire en clair en ne connaissant pas la clé.

# 5. Bibliographie

## *5.1 Techniques de chiffrement*

### 5.1.1 Monographies

**John Vacca** / *Sécurité sur Internet - Secrets* - Sybex - 1996, 938 p., 278 F. - ISBN 1 : 1-56884-457-3 (vers. originale), ISBN 2 : 2-7361-2135-X (vers. française).

**Brian Beckett** / *Introduction aux méthodes de la cryptologie* - trad. de l'anglais par Philippe Béguin, Masson - 1990, 332 p., 24 cm. - ISBN : 2-225-81941-6.

**Xavier Marsault** / *Compression et cryptage des données multimédias* - 2ème ed. revue et augmentée, Paris, Hermès - 1995, 243 p., 24 cm. - ISBN : 2-86601-482-0.

**Olivier Andrieu, Denis Lafont** / *Internet et l'entreprise* - Paris, Eyrolles - sept. 1995, 395 p. - ISBN : 2-212-08906-6.

**Salomaa Arto** / *Introduction à l'informatique théorique : Calculabilité et complexité* - trad. par Alain Deruyver, Paris, A. Colin - 1989, 372 p., 23 cm. - ISBN : 2-200-21063-9.

**Gilles Brassard** / *Cryptologie contemporaine,* trad. par Claude Goutier) - Masson - 1993, 124 p., 24 cm. - ISBN : 2-225-83970-0.

**André Muller** / *Le décryptement* - Paris, P.U.F. - 1983, 127 p., 18 cm., Coll. « Que sais-je ? « n° 2112 - ISBN : 2-13-038020-4.

*Applied cryptography : protocols, algorithms and source code in C* - 2ème éd., New York, John Wiley & sons - 1996, 758 p., 24 cm. - ISBN : 0-471-11709-9.

*ABC de cryptographie avec programmes en Basic* - Masson - 1984, 207 p., 24 cm., ISBN : 2-225-36039-0 (erroné).

**Jean-François Geneste** / *La cryptologie : un monopole ?* - Toulouse, J.-F. Geneste - 1994, 90 p., 30 cm.,150 F. - ISBN 2-9508094-0-5.

**Terry Bernstein, Anish B. Bhimani, Eugène Schultz, Carol A. Siegel** / *Sécurité Internet pour l'entreprise - International Thomson Publishing* - 1996, 425 p., 220 F.

**C. Lidyy** /*Commercial security on the Internet* - Information Management & Computer Security, vol. 4 - 1996, p. 47.9.

### 5.1.2 Périodiques

**Frédéric Métailié** / *Etes-vous un utilisateur authentique ?* - Netsurf, n° 9 - nov. 1996, p. 58-59, 35 F. - ISSN : .1272-9388.

*Objectif Sécurité des réseaux ?* - Informatiques magazine, n° 24 - janv. 1997, p.72-83, 20 F. - ISSN : 1254-8189.

**Olivier Abou, David Jamois-Desautel** / *Sécurité au-delà de la parano sur le Net* - •Net, n° 3 - janv. 1997, p. 44-55, 35 F.

**Serge D. Grun** / *Sécurité* - Internet Professionnel, n° 6 - fév. 1997, p. 18-21, 35 F. - ISSN : 1278-5113.

**Isabelle de Col** / *Cryptographie* - Paris : la Pensée universelle - 1980, 64 p., 18 cm., 20 F. - ISSN 0337-1131.

**Guy Robin** / *Algorithmique et cryptographie* - Paris, Ellipses - 1992, 124 p., 24 cm., 150 F. - ISSN 1154-483X

### 5.1.3 Internet - Les FAQs

***Les « FAQ » (Frequently Asked Questions)***

Université LYON I :

ftp.univ-lyon1.fr/faq/by_name
Mot-clé : crypto

Université de l'Ohio (Etats-Unis, C.I.S.) :

http://www.cis.ohio-state.edu/htbin/search-usenet.faqs
Mot-clé : crypto

### 5.1.4 Internet - Les sites « utiles »

International Cryptographic Software Pages : http://www.cs.hut.fi/crypto
(chiffrement sur le réseau)

CNRS - Michel Dreyfus : http://www.auteuil.cnrs-dir.fr/~dreyfus/infosecu.html
(bulletins d'information)

The Annex : http://www.geocities.com/SiliconValley/6573/index.html
(site de « hackers »)

Quadralay's Cryptography Archive : http://www.austinlinks.com/Crypto/
(Archives américaines sur le sujet)

PGP : http://www.pgp.com
(site du célèbre auteur de PGP)

Travaux du CNAM : http://web.cnam.fr/Network/Crypto
(Utilisation du chiffrement en France)

Logiciel NetCommerce de IBM : http://www.internet.ibm.com
(Logiciel de sécurisation des transactions)

## *5.2 Domaines d'utilisation*

### 5.2.1 Périodiques

**Gilles Pouzin, Thieery Fabre,Gilles Fontaine** / *Entrez dans l'âge du Cybercommerce* - l'Expansion, n° 559 - 19 déc. 1996, p. 66-77 (dossier de 6 articles), 20 F. - ISSN : 0014-4703.

**Charles de Laubier, Pierre Grumberg** / *Commerce électronique c'est parti !* - Le Monde Informatique Magazine, n° 23 - fév. 1997, p. 63-75, 20 F. - ISSN : 0242-5769.

**Stéphane Viossat, François Planque, Claire Pigeassou** / *Tout acheter sur le Web !* - Netsurf, n° 10 - déc. 1996, p. 34-39, 35 F., ISSN : 1272-9388.

**Laurent Pigaud** / *Banque à domicile ? Un rêve* ... - Netsurf, n° 10 - déc. 1996, p. 44-48, 35 F. - ISSN : 1272-9388

### 5.2.2 Monographies

**Les marchands de l'Internet** / *Dominique Hoeltgen*, les éditions du téléphone - 1996, 299 p., 178 F. - ISBN : 2-7976-2341

### 5.2.3 Internet - Les sites « utiles »

Services sécurisés : http://www.globeonline.com
http://www.mondex.com
http://www.buydirect.com
http://www.club-internet.fr

Porte-Monnaie électronique : http://www.digicash.com (Digicash)
http://www.img-inc.com (CyberCash)
http://www.kleline.fr (Kleline)

## *5.3 Aspects juridiques*

### 5.3.1 Monographies

**Valérie Sedallian** / *Droits de l'Internet - Règlementation, responsabilités, contrats* - collection AUI (Association des Utilisateurs d'Internet) - 1996, 336 p., 249 F. - ISBN : 2-9510901-0-2.

### 5.3.2 Périodiques

**Lois et décrets** / *loi n° 96-659 de réglementation des télécommunications,* n° 174 du Journal Officiel (JO) - 27 juill. 1996, p. 11384-11400 - ISSN 0373-0425.

**Pierre Agède** / *Internet : Maîtrisez les risques juridiques* - l'Entreprise, n° 132 - oct. 1996, p. 132-136, 20 F. - ISSN 1164-7027.

**Thierry Parisot** / *Préparatifs avant la grande plongée* - Le Monde Informatique, n° 703 - 20 déc. 1996, p. 40-41, 25 F. - ISSN : 0242-5769.

*Par le petit trou de la serrure* - Planète Internet, n° 14 - déc. 1996, p. 20-21, 30 F. - ISSN 1267-3331.

### 5.3.3 Internet - Les sites « utiles »

Ministère délégué à la poste, aux télécommunications et à l'espace :
http://www.telecom.gouv.fr/francais/activ/telecom/reglemen.htm

CITADEL : http://www.citadeleff.org/crypto
(Site de défense des droits de cryptage)

Projet de loi sur la cryptographie en France : http://www.planete-internet.com/crypto/decret

# 6. Annexe

- CRYPTOLOGIE -

**Propositions SCSSI :**

**Décret définissant les conditions dans lesquelles sont agréés les organismes gérant, pour le compte d'autrui, des conventions secrètes de moyens ou prestations de cryptologie permettant d'assurer des fonctions de confidentialité.**

**Article 1- Définitions.**

**On entend par système de chiffrement à clé symétrique (dit à clé secrète) tout système dans lequel les opérations de chiffrement et de déchiffrement font appel à la même clé.** *Cette clé constitue une convention secrète.*

**On entend par système de chiffrement à clés asymétriques (dit à clés publiques) tout système dans lequel les opérations de chiffrement et de déchiffrement font chacune appel à une clé différente. La clé de chiffrement (dite clé publique) n'a pas à être conservée secrète. La clé de déchiffrement (dite clé privée) doit être conservée secrète.**
**La clé de chiffrement et la clé de déchiffrement forment un couple (dit couple de clés asymétriques) dont les éléments sont dépendants.**
*Ce couple de clés asymétriques constitue une convention secrète.*

**On entend par signature numérique d'un message, l'opération qui consiste à calculer à l'aide d'une clé privée asymétrique, une valeur dépendant de tous les éléments constituant le message. La vérification de la signature fait appel à la clé publique asymétrique correspondante.**

**On entend par code d'authentification d'un message, la valeur dépendant de tous les éléments constituant le message, calculée à l'aide d'une clé symétrique.**
**L'authentification du message est effectuée avec cette clé.**

**On entend par génération de conventions secrètes, la création des clés symétriques ou asymétriques.**

**On entend par certification de conventions secrètes ou de clés publiques, l'opération qui consiste à calculer une signature numérique ou un code d'authentification destinés à prouver leur origine.**

**On entend par publication de clés publiques, l'opération qui consiste à mettre une liste de clés publiques à la disposition des utilisateurs.**

**On entend par gestion de conventions secrètes, la génération, la détention, la certification, la distribution ou la publication des clés nécessaires à la mise en oeuvre d'un moyen ou d'une prestation de cryptologie.**

*E.N.S.S.I.B.*
Ecole Nationale Supérieure
des Sciences de l'Information
et des Bibliothèques

U.C.B.L.
Université
Claude Bernard
LYON I

# Année 1996-1997

Je soussigné, Denis Philippon, auteur du rapport de recherche intitulé :

**Sécurité sur Internet**

**Techniques de chiffrement,
Domaines d'utilisation et
Législation en France**

- Autorise la diffusion du document en l'état.
- ~~Autorise la diffusion du document sous réserve de modifications.~~
- ~~N'autorise pas la diffusion du document.~~

**(Rayer les mentions inutiles)**

le 21 mars 1997 Denis Philippon