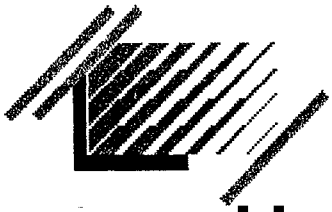
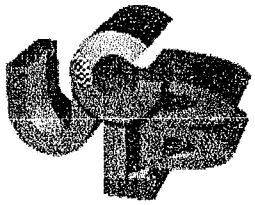


enssib
Ecole Nationale Supérieure
des Sciences de l'Information
et des Bibliothèques



Université
Claude Bernard
Lyon I

DESS Informatique Documentaire

Rapport de recherche bibliographique

Les algorithmes de cryptologie

Philippe PEREZ

Sous la direction de

Monsieur Omar LAROUK

Institut Universitaire de Technologie de Dijon

Année 1999

Les algorithmes de cryptologie

Philippe PEREZ

Résumé : Utilisée pour la sécurité dans les domaines de l'information et des communications, la cryptologie est l'ensemble des techniques permettant de transcrire une information compréhensible en une information incompréhensible par l'application d'algorithmes.
Ce rapport présente un état de l'art en la matière ainsi que les aspects juridiques de la législation française.
Une bibliographie thématique est proposée à la fin.

Descripteurs : ALGORITHME, CRYPTOLOGIE, CRYPTAGE, CRYPTOGRAPHIE, CHIFFREMENT, SECURITE INFORMATIQUE, LEGISLATION FRANÇAISE, LOI

Title : The algorithms of cryptology

Abstract : Used for security in the computeur science and communication domains, cryptology is all technics which allow to transcribe understandable information into non-understandable information using algorithms.
This report presents a state of art about cryptology as well as the juridic aspects of the French legislation.
A thematic bibliography is included at the end.

Keywords : ALGORITHM, CRYPTOLOGY, ENCRYPTION, CRYPTOGRAPHY, COMPUTER SCIENCE SECURITY, FRENC LEGISLATION, LAW

TABLE DES MATIERES

« Il faut considérer la bibliographie comme la possibilité de résoudre,
sinon une énigme, au moins un problème ».

Guide de la bibliographie générale.

« Désignant aussi bien une donnée de base qu'un document élaboré,
un instrument de travail qu'une technique de rédaction,
la bibliographie nous semble être surtout une méthode logique d'investigation
documentaire dont le but est d'élaborer une information précise... qui à la fois
soutient et justifie un travail intellectuel et lui permet de progresser en lui
indiquant des voies nouvelles. »

J. ARCHIMBAUD, 1970.

1. Introduction

1.1. Définition de la mission

Monsieur Omar Larouk, Maître de Conférences à l'Institut Universitaire de Technologie de Dijon et à l'Ecole Nationale Supérieure des Sciences de l'Information et des Bibliothèques (E.N.S.S.I.B.) de Villeurbanne, m'a demandé d'établir un rapport de recherche bibliographique sur le thème des **algorithmes de cryptologie**.

L'objet de cette recherche est d'obtenir une *bibliographie courante* et *rétrospective*[1] recensant des documents en langue française ou anglaise. Elle devra permettre de présenter et de décrire les différents algorithmes utilisés dans le domaine de la cryptologie, de définir leurs utilités, leurs domaines d'application et de connaître les aspects juridiques dans la législation française.

1.2. Problématique de recherche

Quel que soit le support de recherche utilisé (CD-ROM, base de données, internet, logiciel documentaire, ...), l'accès à l'information se faisant par le *langage documentaire à structure combinatoire*, il est extrêmement important de bien choisir les mots-clés (ou critères) afin de réduire le *silence* et le *bruit*.

En analysant rapidement la question, il semblerait évident d'utiliser les critères **algorithme**, **cryptologie**, auxquels on rajouterait leur traduction en anglais **algorithm** et **cryptology**.

Toutefois, cette analyse serait insuffisante, car il convient de résoudre certains problèmes tels que la synonymie ou la syntaxique.

Si les mot **algorithme** ou **algorithm** n'ont pas de synonyme, les mots **chiffrement**, **cryptage**, **encryptage**, **cryptographie**, **cryptologie** pour le français et **encryption**, **cryptography**, **cryptology** pour l'anglais sont souvent utilisés pour signifier la même chose.
D'autre part, le mot **algorithme** pris tout seul est trop général. En effet il existe plusieurs sortes d'algorithmes : de cryptage, de compression, de programmation, de traitements, ou encore, qui portent le nom de leurs créateurs : d'Huffman, de Shannon, de Kruskal, de Prim, etc. Il ne pourra donc en aucun cas être utilisé comme unique critère de recherche.

Si les moteurs de recherche permettent souvent les troncatures, elles devront ici être utilisées avec précaution. En effet, si **algorithm***, qui prendrait en compte les mots **algorithmie**, **algorithmique**, n'aurait pas une grosse influence sur le sens de la recherche, les troncatures **crypt*** ou **crypto***[2] auraient pour effet de prendre en compte des mots de nature totalement différente tels que CRYPTE, CRYPTIQUE, CRYPTOCHIDIE, CRYPTOGAME, CRYPTOGENETIQUE, CRYPTOMERIA, CRYPTOZOOLOGIE, et bien d'autres.

Pour toutes ces raisons, les **troncatures utilisées ne couvriront que les pluriels des mots et les suffixes** qui diffèrent entre le français et l'anglais.

2. Recherche bibliographique

La recherche a été réalisée à partir des **CD-ROM** installés sur le serveur de CD-ROM de l'E.N.S.S.I.B., des bases de données **Inside** de la **British Library** et du serveur **Dialog**, des **bibliothèques** et d'**internet**.

---

[1] Les mots en italiques sont définis dans le glossaire
[2] Crypto : du grec " cryptein ", cacher, ajoute une notion de clandestinité au mot source.

1.1. Recherche sur CD-ROM

2.1.1. Stratégie de recherche

Quel que soit le CD-ROM utilisé, la recherche peut être effectuée à partir d'une liste de mots-clés (index). Cela a l'avantage d'assurer que le mot-clé sélectionné retourne au moins une réponse.

2.1.2. Base de données BNF

Le CD-ROM de la Bibliothèque Nationale de France (B.N.F.) contient 800 000 notices bibliographiques d'ouvrages entrés par dépôt légal depuis 1970. Cela concerne tous les types de documents édités, imprimés ou diffusés sur le territoire français.

La recherche a été effectuée par SUJET avec les mots-clés proposés dans l'index.

Equation de recherche	Résultats obtenus	Résultats pertinents	Taux de pertinence[3]
"CRYPTAGE" OU "CRYPTAGE INFORMATIQUE" OU "CHIFFREMENT INFORMATIQUE" OU "ENCRYPTAGE INFORMATIQUE"	30	8	27 %

La notice ne contenant pas de résumé, la *pertinence* des résultats a été déterminée en fonction du titre.

2.1.3. Base de données DOCTHESES

Ce CD-ROM dépend de l'Agence Bibliographique de l'Enseignement Supérieur (ABES) basée à Montpellier. Il recense les notices de thèses de doctorat soutenues dans les universités françaises. Il inclut les thèses de lettres, sciences humaines et sociales depuis 1972, de santé depuis 1983, et des sciences vétérinaires depuis 1991.

La recherche a été effectuée par MOTS-CLES issus de l'index.

Equation de recherche	Résultats obtenus	Résultats pertinents	Taux de pertinence
CRYPTOGRAPHIE OU CRYPTAGE OU CHIFFREMENT	30	4	13 %

La *pertinence* des résultats a été déterminée en fonction du titre et du résumé.

[3] Le taux de pertinence est le rapport entre les résultats pertinents des les résultats obtenus.

2.1.4. Base de données ELECTRE

Il s'agit de la base de données bibliographique du Cercle de la Librairie contenant des renseignements sur les éditeurs et sur les diffuseurs. Elle contient 400 000 titres depuis 1986.
Cela concerne notamment des livres édités par les éditeurs français en toutes langues ou par les éditeurs étrangers en français.

La recherche a été effectuée par SUJET avec les mots-clés proposés dans l'index.

Descripteurs	Résultats obtenus	Résultats pertinents	Taux de pertinence
CHIFFREMENT	3	1	33 %
CRYPTOGRAPHIE	12	5	42 %

La notice ne contenant pas de résumé, la pertinence des résultats a été déterminée en fonction du titre.

2.1.5. Base de données LISA PLUS

Le CD-ROM Library and Information Science Abstracts Plus est établi par la Library Association et par l'ASLIB, deux associations professionnelles anglaises. Il inclut tout type de documents. C'est la base spécialisée en sciences de l'information et bibliothéconomie.

La recherche a été effectuée par MOTS-CLES issus de l'index.

Equation de recherche	Résultats obtenus	Résultats pertinents	Taux de pertinence
CRYPTOGRAPHY OR CRYPTOLOGY OR ENCRYPTION	12	3	25 %

La pertinence des résultats a été déterminée en fonction du titre et du résumé.

2.2. Recherche sur Dialog

2.2.1. Stratégie de recherche

Devant la multiplicité du nombre de bases sous le serveur Dialog, le problème est de savoir quelles sont celles qui répondront au mieux à la question posée.

Pour cela, l'utilisation de la base DIALINDEX (numéro 411) permet une recherche sur une collection de bases.
La cryptologie concernant la sécurité informatique, c'est la catégorie Computer Science (COMPSCI) qui a été retenue.

La recherche devant aboutir sur une *bibliographie courante* et *rétrospective*, il n'a été effectué aucune limitation sur la date de publication. Seule une limitation au niveau de la langue a été établie, les documents devant être en anglais ou en français.

2.2.2. Mots-clés et troncatures

Comme il a été énoncé précédemment, les troncatures utilisées permettent de couvrir les pluriels des mots et les suffixes qui diffèrent entre le français et l'anglais.

MOT-CLE ET TRONCATURE	COMMENTAIRE
ALGORITHM??	Les 2 points d'interrogation sans espace permettent 0,1 ou 2 caractères après le mot. En effet, en français on peut trouver ALGORITHME ou ALGORITHMES et en anglais ALGORITHM ou ALGORITHMS.
ENCRYPTION? ?	Les 2 points d'interrogation espacés permettent 0 ou 1 caractère après le mot. Cette troncature permettra l'éventuel pluriel de ce mot anglais.
CRYPTOLOG??	Les 2 points d'interrogation sans espace supportent le mot français CRYPTOLOGIE et de son équivalent en anglais CRYPTOLOGY.
CRYPTOGRAPH??	Les 2 points d'interrogation sans espace supportent le mot français CRYPTOGRAPHIE et de son équivalent en anglais CRYPTOGRAPHY.
CHIFFREMENT? ?	Un caractère supplémentaire pour supporter un éventuel pluriel.
CRYPTAGE? ?	Un caractère supplémentaire pour supporter un éventuel pluriel.

2.2.3. Les opérateurs

La recherche sous Dialog accepte tous les types d'opérateurs : booléen et de proximité. C'est opérateurs sont exprimés en anglais.

Les opérateurs décrits ci-dessous sont ceux utilisés pour la recherche.

OPERATEURS UTILISES	DEFINITION
AND	Opérateur booléen retournant tous les enregistrements contenant tous les termes de la recherche. Intersection.
OR	Opérateur booléen retournant tous les enregistrements contenant au moins un des termes de la recherche. Union.
(1N)	Opérateur de proximité retournant les termes espacés de 0 ou 1 caractère dans les deux sens. Exemple : ALGORITHM??(1N)CRYPTOLOG?? retourne : ALGORITHME DE CRYPTOLOGIE ou CRYPTOLOGY ALGORITHMS

2.2.4. Détail de la recherche

2.2.4.1. Utilisation de DIALINDEX

COMMANDE	COMMENTAIRE
B 411	Ouverture de la base DIALINDEX
SF COMPSCI	Ouverture des bases de la collection Computer Science

DIALINDEX - RECHERCHE NUMERO 1

Aucune restriction sur les champs n'a été effectuée. La recherche a donc porté sur les champs : TITRE - DESCRIPTEUR - RESUME

S algorithm?? AND encryption? ? AND cryptolog?? AND cryptograph?? AND cryptage? ? AND chiffrement? ?

Bien que cette recherche soit trop restrictive, elle a néanmoins permis de rapidement vérifier que chaque mot-clé avec sa troncature retourne au moins une réponse dans au moins une base de données.

DIALINDEX - RECHERCHE NUMERO 2

Aucune restriction sur les champs n'a été effectuée.

S algorithm?? AND (encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?)

Cette recherche, plus affinée, a permis de définir si toutes les bases de la catégorie COMPSCI retourne au moins une réponse. Ceci afin d'effectuer une sélection sur le choix de ces bases.

Après avoir listé les réponses par ordre croissant du nombre de réponses grâce à la saisie de la commande **RF** (RANK FILE), il a été constaté que toutes les bases retournent au moins une réponse.

2.2.4.2. Utilisation de ONESEARCH

OneSearch permet une recherche sur plusieurs bases à la fois. Le choix de ces bases devait dépendre des résultats obtenus dans la recherche par Dialindex. Toutefois, dans un premier temps, il a été décidé de n'exclure aucune base de la catégorie COMPSCI. En effet, ce sont les équations de recherche choisies qui permettront d'« exclure » les bases de données susceptibles de ne retourner aucune réponse.
Une première extraction permettra d'analyser les résultats obtenus. Si le nombre de résultats retournés est inexploitable (trop grand nombre de références) ou incohérent (après analyse de l'extraction : titre, résumé, descripteurs), une sélection des bases de données les plus représentatives (d'après les résultats obtenus sous la base DIALINDEX après la commande RF) sera effectuée.

ONESEARCH - RECHERCHE NUMERO 1

Aucune restriction sur les champs n'a été effectuée. La recherche a donc porté sur les champs : TITRE - DESCRIPTEUR - RESUME

S algorithm?? AND (encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?)

Résultat de la recherche : 9505 références obtenues

Le résultat est quasiment inexploitable du fait du trop grand nombre de références obtenues.
Afin de réduire le nombre de réponses, l'opérateur de proximité (1N) remplacera l'opérateur Booléen AND.
En effet, l'opérateur de proximité (1N) autorise 0 ou 1 terme entre les mots. Il permettra de retrouver les chaînes indépendamment du langage anglais ou français : ALGORITHME(S) DE CRYPTAGE, ALGORITHME(S) DE CRYPTOLOGIE, ENCRYPTION ALGORITHMS, CRYPTOGRAPHIC ALGORITHM, etc...

ONESEARCH - RECHERCHE NUMERO 2

Aucune restriction sur les champs n'a été effectuée. La recherche a donc porté sur les champs :
TITRE - DESCRIPTEUR - RESUME

S algorithm??(1N)(encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?)

Résultat de la recherche : 2903 références obtenues

Le nombre de réponses a diminué de plus de deux tiers par rapport à la recherche précédente.
Toutefois, le nombre de réponses obtenues est encore trop grand.
Afin de distinguer les références anglaises et françaises, on va effectuer une restriction au niveau de la langue.

ONESEARCH - RECHERCHE NUMERO 3

Aucune restriction sur les champs n'a été effectuée. La recherche a donc porté sur les champs :
TITRE - DESCRIPTEUR - RESUME

S algorithm??(1N)(encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?) AND LA=FRENCH

Résultat de la recherche : 15 références obtenues

Ce nombre de réponses indique le peu de références en langue française sur Dialog.

Les 15 références ont été extraites.

ONESEARCH - RECHERCHE NUMERO 4

Aucune restriction sur les champs n'a été effectuée. La recherche a donc porté sur les champs :
TITRE - DESCRIPTEUR - RESUME

S algorithm??(1N)(encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?) AND LA=ENGLISH

Résultat de la recherche : 2613 références obtenues

Le nombre de réponses obtenues est trop important pour être exploitable.
Afin de le diminuer, on va effectuer une recherche uniquement sur le titre.

ONESEARCH - RECHERCHE NUMERO 5

La recherche est effectuée sur le champ : TITRE

S (algorithm??(1N)(encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?) AND LA=ENGLISH) **/TI**

Résultat de la recherche : 288 références obtenues

Le résultat obtenu est intéressant. On va toutefois essayer de le diminuer en effectuant une recherche sur les descripteurs.

ONESEARCH - RECHERCHE NUMERO 6

La recherche est effectuée sur le champ : DESCRIPTEUR

Pour cette recherche, l'opérateur AND a été préféré au (1N) car les descripteurs constituent souvent une liste non ordonnée. Ainsi, l'opérateur (1N) ne retournerait pas les références dont les termes seraient espacés de plus d'un mot.

S (algorithm?? AND (encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?) AND LA=ENGLISH) **/DE**

Résultat de la recherche : 5882 références obtenues

Le résultat obtenu est normal compte tenu que seule la recherche sur le titre avait permis d'obtenir un résultat exploitable.

ONESEARCH - RECHERCHE NUMERO 7

La recherche est effectuée sur le champ : TITRE et DESCRIPTEUR

Le but de cette recherche est d'effectuer la concaténation des deux dernières recherches (5 et 6).

S ((algorithm??(1N)(encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?) AND LA=ENGLISH) **/TI**)
AND
((algorithm?? AND (encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?) AND LA=ENGLISH) **/DE**)

Résultat de la recherche : 227 références obtenues

L'objectif qui avait été défini après la recherche 5 est atteint : imposer la présence des mots du titre dans les descripteurs a permis d'obtenir un résultat plus fin.

Après suppression des doublons par la commande REMOVE DUPLICATES (RD), on obtient :

132 références

Afin d'avoir un aperçu des résultats obtenus, une extraction des 15 premières références a été effectuée.
Après analyse des titres, résumés et descripteurs, nous avons constaté **un défaut dans la démarche**. En effet, la requête portant sur les titres avec l'opérateur (1N) (OneSearch - Recherche numéro 5) ne retourne pas les références spécialisées dans un algorithme en particulier (DES, RSA, IDEA, etc...).
Afin de remédier à ce problème, **l'opérateur (1N) sera remplacé par un OR**.
Cette nouvelle démarche devant obligatoirement ramener un nombre plus important de résultats, il a été décidé de limiter le nombre de bases interrogées à 4. Cette sélection a été effectuée grâce aux résultats obtenus dans la base DIALINDEX après la commande RF.

En effet, les résultats obtenus étaient les suivants :

N1	828	275: IAC(SM) Computer Database(TM)_1983-1999/Feb 02
N2	468	2: INSPEC_1969-1999/Jan W4
N3	381	8: Ei Compendex(R)_1970-1999/Jan W5
N4	185	144: Pascal_1973-1998/Dec
N5	96	674: Computer News Fulltext_1989-1999/Jan W5

...

Après avoir consulté le lexique (BlueSheets) sur Internet, nous avons constaté que les 4 bases sélectionnées :

- Couvrent les principaux types de *documents primaires* : périodiques, livres, thèses, congrès et brevets
- Pour les restrictions sur les champs TITRE, RESUME, DESCRIPTEUR et la LANGUE, les 4 bases utilisent les même termes : /TI, /AB, /DE, /LA.

L'accès aux bases par la commande OneSearch sera donc **B 275,2,8,144**

ONESEARCH - RECHERCHE NUMERO 8

Aucune restriction sur les champs n'a été effectuée. La recherche a donc porté sur les champs : TITRE - DESCRIPTEUR - RESUME

B 275,2,8,144

S algorithm?? AND (encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?)

Résultat de la recherche : 5771 références obtenues

ONESEARCH - RECHERCHE NUMERO 9

Aucune restriction sur les champs n'a été effectuée.

S algorithm??(1N)(encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?)

Résultat de la recherche : 2028 références obtenues

ONESEARCH - RECHERCHE NUMERO 10

Aucune restriction sur les champs n'a été effectuée

S algorithm??(1N)(encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?) AND LA=ENGLISH

Résultat de la recherche : 1833 références obtenues

ONESEARCH - RECHERCHE NUMERO 11

Cette recherche constitue la nouvelle démarche avec exclusivement des opérateurs OR.

Devant l'importance du nombre de domaines qui le concerne, le descripteur **algorithm??** a été abandonné. Cette éviction qui n'a pour but que d'éviter le *bruit* n'aura pas d'importance au niveau du résultat final, car les recherches sur le résumé et les descripteurs contiendront toujours le terme.

S encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?

Résultat de la recherche : 28886 références obtenues

Le résultat obtenu était prévisible. Il ne sera exploitable que combiné avec les autres résultats.

ONESEARCH - RECHERCHE NUMERO 12

La recherche a porté sur le champ : TITRE

S (encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?) AND LA=ENGLISH **/TI**

Résultat de la recherche : 5105 références obtenues

Le nombre de références obtenues a été multiplié par presque 25 par rapport à celui avec l'opérateur (1N) de la recherche numéro 5 (5105 contre 208 réponses). Ce résultat est normal car la recherche précédente comportait un descripteur supplémentaire qui, de plus, se combiné avec un opérateur de proximité.

ONESEARCH - RECHERCHE NUMERO 13

La recherche a porté sur le champ : DESCRIPTEUR

S (algorithm?? AND (encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?) AND LA=ENGLISH) **/DE**

Résultat de la recherche : 5882 références obtenues

ONESEARCH - RECHERCHE NUMERO 14

Cette recherche constitue une nouvelle démarche avec une restriction sur le RESUME.

La recherche n° 5 imposait la proximité entre les descripteurs par l'opérateur (1N). Afin de garder l'assurance que l'on parle bien d'algorithme de chiffrement, de cryptologie, etc., cette recherche va être « déplacée » au niveau du résumé. Cela permettra aussi d'effectuer une restriction supplémentaire, afin de ne pas avoir, à la fin, beaucoup trop de références.

S (algorithm??(1N)(encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?) AND LA=ENGLISH) **/AB**

Résultat de la recherche : 784 références obtenues

ONESEARCH - RECHERCHE NUMERO 15

Cette recherche est la concaténation des trois dernières recherches (12, 13 et 14).

S ((encryption? ? OR cryptage? ? OR cryptolog?? OR
cryptograph?? OR chiffrement? ?) AND LA=ENGLISH) **/TI**)
AND
((algorithm??(1N)(encryption? ? OR cryptage? ? OR cryptolog?? OR
cryptograph?? OR chiffrement? ?) AND LA=ENGLISH) **/AB**)
AND
((algorithm?? AND (encryption? ? OR cryptage? ? OR cryptolog?? OR
cryptograph?? OR chiffrement? ?) AND LA=ENGLISH) **/DE**)

Résultat de la recherche : 315 références obtenues

Après suppression des doublons par la commande REMOVE DUPLICATES (RD), on obtient :

238 références

Comme on l'avait pressenti , cette deuxième démarche a retourné plus de références. Toutefois, ce résultat reste exploitable. Pour des raisons de coûts, seules les 100 premières références ont été extraites.

Afin de résumer toutes les équations de recherche effectuées ainsi que les résultats obtenus, les pages suivantes proposent un récapitulatif sous la forme de tableaux.

2.2.4.3. Récapitulatif des résultats sur DIALOG

B COMPSCI

Numéro de recherche	Recherche	Résultats obtenus
S1	S algorithm?? AND (encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?)	9505
S2	S S1 AND LA=ENGLISH	8461
S3	S algorithm??(1N)(encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?)	2903
S4	S S3 AND LA=ENGLISH	2613
S5	S S4/TI	288
S6	S S2/DE	5882
S7	S S5 AND S6	227
S8	RD S7	**132**
S9	S S3 AND LA=FRENCH	**15**

Les 15 références en langue française ont été extraites.

Afin de vérifier la pertinence des résultats obtenus sur quelques références, les 10 premières références en langue anglaise avaient été extraites.
On avait alors constaté qu'aucun des documents ne concernait un algorithme en particulier. Dans beaucoup de résumés, les algorithmes étaient appelés par leur nom. En effet, pour un initié, parler du DES ou du RSA ou d'IDEA signifie implicitement de parler d'algorithmes de cryptologie. Aussi, afin de pouvoir obtenir des références ayant pour titre le nom d'un algorithme, une nouvelle démarche avait été instaurée.

B 275,2,8,144

Numéro de recherche	Recherche	Résultats obtenus
S1	S algorithm?? AND (encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?)	5771
S2	S S1 AND LA=ENGLISH	5266
S3	S algorithm??(1N)(encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?)	2028
S4	S S3 AND LA=ENGLISH	1833
S5	S encryption? ? OR cryptage? ? OR cryptolog?? OR cryptograph?? OR chiffrement? ?	28886
S6	S S5 AND LA=ENGLISH	25988
S7	S S6/TI	5105
S8	S S2/DE	3561
S9	S S4/AB	1833
S10	S S7 AND S8 AND S9	315
S11	RD S10	**238**

2.2.5. Etude de la pertinence des résultats

115 références (100 en anglais et 15 en français) ont été extraites. La pertinence a été exprimée en fonction du titre et du résumé.

REFERENCE EN FRANCAIS			REFERENCE EN ANGLAIS		
Résultats obtenus	**Résultats pertinents**	**Taux de pertinence**	**Résultats obtenus**	**Résultats pertinents**	**Taux de pertinence**
100	78	78 %	15	7	40 %

2.2.6. Conclusion

Le nombre de références sur ce thème étant extrêmement important, il convenait de choisir une démarche restrictive afin d'éviter un trop grand nombre de références.

Le choix d'effectuer des restrictions sur le TITRE, le RESUME et sur les DESCRIPTEURS avec les opérateurs AND et (1N) a permis d'obtenir un nombre de réponses que l'on peut exploiter. En effet, il n'est pas bon d'avoir trop de références si l'on ne les extrait pas toutes, car rien ne signifie que la partie extraite contient les meilleures références.

2.3. Recherche sur la base Inside de la British Library

La Bristish Library a donné la possibilité de tester sa base pendant environ un mois entre janvier et février 1999. Cette base est accessible sur internet sur le site http://inside.bl.uk:443.

2.3.1. Stratégie de recherche

La base Inside contient l'ensemble des collections de la British Library, soit environ 20 000 titres de revues courantes de par de monde, 70 000 titres de conférences, 250 000 titres de journaux couvrant un période de plus de 300 ans.

Afin de minimiser le bruit, c'est la technique de recherche « Text Searching » qui a été privilégiée. C'est la seule permettant une *recherche évoluée* sur la base entière par saisie de mots-clés.

2.3.2. Résultats obtenus

Equation de recherche	Résultats obtenus	Résultats pertinents	Taux de pertinence
Chiffrement	1	0	0 %
Cryptage	1	0	0 %
algorithm$ **AND** (encryption **OR** cryptolog$ **OR** cryptograph$)	319	-	-
algorithm$ **NEAR1** (encryption **OR** cryptolog$ **OR** cryptograph$)	70	13	21 %

Grâce à la recherche évoluée, l'opérateur NEAR1 a réduit de 78 % le nombre de réponses avec l'opérateur AND.

La base ne fournissant que très peu de résumés, la pertinence des résultats a été déterminée en fonction du titre.

Sur les 13 résultats pertinents, il y a :

- 5 articles de conférences
- 7 articles de périodiques

2.4. Recherche dans les bibliothèques

2.4.1. Stratégie de recherche

La recherche a été effectuée à partir du catalogue des bibliothèques.

2.4.2. Catalogue de la bibliothèque de l'E.N.S.S.I.B.

La recherche a été effectuée par MOTS DU TITRE ET DU SUJET.

Equation de recherche	Résultats obtenus	Résultats pertinents	Taux de pertinence
algorithm* ET crypt*	0	0	-
cryptolog* OU cryptag* OU chiffrement	3	2	67 %

La pertinence des résultats a été déterminée en fonction du titre.

2.4.3. Catalogue de la bibliothèque universitaire de LYON I

La recherche a été effectuée sur les MOTS-CLES.

Equation de recherche	Résultats obtenus	Résultats pertinents	Taux de pertinence
chiffrement	0	0	-
cryptologie	2	2	100 %
cryptographie	10	6	60 %

La pertinence des résultats a été déterminée en fonction du titre.

2.4.4. Catalogue de la base de Doc'INSA.

La recherche a été effectuée sur internet[4].

Utilisation de la recherche experte des livres, thèses, congrès et rapports de Doc'INSA à partir de l'index général.

Equation de recherche	Résultats obtenus	Résultats pertinents	Taux de pertinence
algorithm* AND (cryptage OR chiffrement OR cryptologie OR cryptographie)	6	4	67 %

La pertinence des résultats a été déterminée en fonction du résumé.

[4] http://csidoc.insa-lyon.fr

2.5. Recherche sur Internet

2.5.1. Stratégie de recherche

La recherche sur internet est d'une toute autre nature que celles citées précédemment. Le principe est l'indexation en texte intégral où tous les mots d'une page web sont indexés par des robots d'exploration.
Ce système possède au moins un avantage et un inconvénient. L'avantage de la recherche plein texte est que l'on peut rechercher une chaîne précise (entre guillemets) : plus besoin d'opérateurs booléen ou de proximité. Par contre, elle interdit les troncatures, les synonymes et les recherches multi-langue. De plus, tous les mots étant des index, une page peut contenir tous les termes recherchés, mais à des endroits tellement éloignés, qu'ils n'ont rien à voir entre eux.

Pour notre recherche, nous utiliserons tous les moyens mis à la disposition sur internet : les moteurs de recherche et méta-moteurs, et les annuaires.

Ces moyens sont réunis sur la page <http://www.adbs.fr/adbs/viepro/sinfoint/lardy/outils.htm>.

2.5.2. Recherche sur Altavista

Altavista a été lancé par la Digital Equipment en décembre 1995. Il est le plus complet des moteurs de recherche et effectue une indexation en texte intégral. Sa base possède plus de 110 millions de pages. Il dispose de plus d'une interface avancée, permettant des requêtes fines et précises avec des opérateurs booléens et de proximité.

Recherche n° 1 (recherche simple)

+algorithm* +(encryption cryptage cryptolog* cryptograph* chiffrement)

72 260 réponses.

Cette recherche contient beaucoup trop de bruit et beaucoup d'*URL* renvoient l'erreur 404 (inexistante).

Recherche n° 2 (recherche avancée)

algorithm* AND (encryption* OR cryptage* OR cryptolog* OR cryptograph* OR chiffrement)

22 607 réponses.

Recherche n° 3 (recherche avancée)

algorithm* NEAR (encryption* OR cryptage* OR cryptolog* OR cryptograph* OR chiffrement)

22 531 réponses.

Afin de limiter le nombre de réponses, une restriction au niveau de la date a été effectuée.
En effet, on peut considérer qu'un site est « vivant » s'il est régulièrement mis à jour. Les sites qui n'auront pas été mis à jour depuis plus d'un an seront exclus. En ce qui concerne la cryptologie, ce délai est plus que raisonnable compte tenu des évolutions incessantes, des besoins grandissants et de l'actualité dans ce domaine.

Ainsi, une limitation de recherche sur la date au 01/Jan/98 a permis de diminuer par 2 le nombre de réponses, soit 11 616 réponses.

Ce nombre encore trop important a encore pu être diminué grâce à l'option **REFINE** et **GRAPH** permettant de sélectionner ou d'exclure des mots tels que authentification, compression, unreable, server, sender, electronic, repudiation, smart, networks, etc...

Le nombre de réponses trouvées a été de 354 pages.

Autres recherches :

Recherche n° 4 (recherche avancée)

LANGUE : **FRENCH**

RANK : **législation**

EXPRESSION BOOLEEN : **algorithm* AND (encryption* OR cryptage* OR cryptolog* OR cryptograph* OR chiffrement)**

91 réponses.

Recherche n° 5 (recherche avancée)

LANGUE : **FRENCH puis ANY LANGUAGE**

EXPRESSION BOOLEEN : **title :algorithm* AND (encryption* OR cryptage* OR cryptolog* OR cryptograph* OR chiffrement)**

Cette recherche sur le titre a retourné 5 réponses pour la langue française et 52 réponses pour toutes les langues.

2.5.3. Recherche sur les autres moteurs et méta-moteurs

La recherche a été effectuée principalement sur les moteurs Yahoo France et International, Voilà, Goto, Nomade et sur les méta-moteurs MetaCrawler et Debriefing.

Tous les moteurs ne permettant pas la recherche avancée, les moyens de recherche ont été :

- Les recherches plein-texte en français ou en anglais telles que : **« algorithmes de cryptage » / « algorithmes de cryptologie » / « description des algorithmes de cryptage » / « législation française [en matière de / sur la] cryptologie » / « l'algorithme RSA » / « PGP en français » /** etc...

- Les recherches simples avec l'énumération des descripteurs telles que : **+algorithm* +encryption / +pgp +zimmermann / +algorithm* +rsa +des +idea** / etc.

- Les recherches combinées (plein-texte et simples ou avancées telles que : **« la législation française » NEAR (cryptologie chiffrement) / +« liste des algorithmes de » +(chiffrement cryptologie cryptographie cryptage) / +« le DES » +ibm** / etc.

- Les recherches sur les URL : **url:crypto / url:rsa / url:pgp / +url:.edu +...** (pour la recherche des sites des écoles et universités américaines) / etc.

Le nombre de réponses a varié selon la recherche. L'option de visite du site a été déterminée à partir des critères suivant :

- le nom du site : certaines URL telles que geocities, altern, multimania, etc... sont des sites d'accueil destinés au public. Ce ne sont donc pas des sites référencés. Leur information n'est donc pas toujours fiable et souvent ces adresses retournent l'erreur 404. Les meilleurs de ces sites sont parfois référencés par des sites plus importants. Leur accès pourra être fait à partir d'un lien d'un site référencé.
- le début de la page : présenté en quelques lignes après le nom du site dans les moteurs de recherche
- le pourcentage de pertinence : selon les moteurs de recherche
- le classement : les moteurs de recherche ordonnent les résultats selon la fréquence des mots trouvés. Les premières réponses sont souvent les plus pertinentes.
- la date de mise à jour affichée par les moteurs de recherche : les sites dont la dernière mise à jour daté de plus d'un an n'ont pas été visités (à l'exception des requêtes pour la législation française en matière de cryptologie).

2.5.4. Les annuaires

Les annuaires proposent des adresses génériques de serveurs web (page d'accueil). Cela évite ainsi l'accès à une page particulière.

La recherche a porté sur les annuaires : Yahoo et Yahoo France, Magellan, Nomade, Hachette Net, Eurêka.

Les sites contenus sont classés par thèmes. Selon l'annuaire utilisé les termes diffèrent. La recherche a porté sur les thèmes tels que : INFORMATIQUE ET MULTIMEDIA, INFORMATIQUE, SECURITE ET CRYPTAGE.

2.5.4.1. Utilisation des liens

Les meilleurs sites proposent des liens : sur d'autres sites, des F.A.Q. (Frequently Asked Questions), les News (forums de conférences).
La visite de ces liens a permis de découvrir d'autres sites qui eux même ont des liens que l'on va aussi visiter... (c'est la toile d'araignée !).

2.6. Critique de la recherche

La difficulté de cette recherche est que le sujet comporte une multitude de références et de sites sur internet. De ce fait, quelle que soit l'équation de recherche, il y avait beaucoup de réponses.

Les CD-ROM offrent l'avantage de proposer un index des descripteurs. De ce fait, le risque de passer à côté de mots-clés est minimisé. Par contre certaines bases n'offraient pas de résumé, ce qui rend l'analyse de la pertinence plus difficile.

Dialog contient beaucoup de bases, et il n'est pas toujours évident de savoir lesquelles sont susceptibles de retourner le plus grand nombre ou les meilleures références.
Paradoxalement, pour notre sujet, le nombre de références présentent dans les bases est bien trop important. Aussi, la visualisation payante des références ne nous permettant pas de tout extraire, rien ne nous assurera que les références visualisées sont les meilleures parmi toutes celles que les bases contenaient.
Pour toutes ces raisons, je pense qu'une recherche très éclectique, sur tout type de documents, dans un domaine très courant (une recherche de type état de l'art) est à proscrire sur Dialog.

L'inconvénient de la recherche plein-texte sur internet est que certaines équations de recherche ont retourné jusqu'à 80 000 réponses. De plus, les bases de données des moteurs de recherche n'étant pas mises à jour, beaucoup d'URL n'existaient plus (erreur 404). Enfin, beaucoup de sites américains étaient des sites commerciaux ou publicitaires sur la sécurité informatique.
Devant le nombre important de sites dans ce domaine, seuls les annuaires ont permis l'accès à des sites intéressants, qui de part les liens qu'ils proposent, permettent d'accéder à d'autres sites, etc., etc.

2.7. Coût de la recherche et temps de travail

2.7.1. Temps

Certains temps affichés sont une approximation.

Type de recherche	Durée (heure)
Recherche sur CD-ROM	4
Recherche sur Dialog	0 h 50
Recherche sur internet	32
Recherche dans les bibliothèques	3
Lectures	48
TOTAL	**87 h 50**

2.7.2. Coût financier

Le coût ne concerne que la consultation des bases de données sur Dialog.

$6.32 Estimated total session cost 3.646 DialUnits
$5.76 Estimated total session cost 2.855 DialUnits
TOTAL : 12.08 $, soit environ 72 francs.

3. Synthèse

3.1. Introduction

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 réaliser l'opération inverse » *(Loi n° 90-1170 sur la réglementation des télécommunications, J.O. du 30/10/94)* [115].
Elle est donc l'art d'écrire des messages sous forme codée [9] et a pour objectif de protéger la confidentialité et l'*intégrité des données*[5].
Vielle depuis l'antiquité, elle permet de communiquer de façon confidentielle par l'entremise des voies de communication susceptibles d'espionnage. Son intérêt commercial est récent et est apparu lors de la révolution industrielle en informatique et dans les télécommunications [2] [4].

3.2. Les principes de base

Supposons qu'un expéditeur veuille transmettre un message à un destinataire et veut être sûr que personne ne pourra agir sur le message de quelque façon que ce soit. Le message appelé ***texte en clair*** doit suivre un processus de transformation appelé ***chiffrement*** (ou ***cryptage***) de telle manière à le rendre incompréhensible . Le résultat de ce processus de chiffrement est appelé ***texte chiffré*** (ou ***cryptogramme***). Le processus de reconstruction du texte en clair à partir du texte chiffré est appelé ***déchiffrement*** (ou ***décryptage***) [13]. Ces différents processus sont illustrés par la figure ci-dessous :

L'art de concevoir ces processus s'appelle la ***cryptographie***. Elle est pratiquée par des **cryptographes** . La branche mathématique qui traite la cryptographie est la ***cryptologie***. Ces pratiquants appelés des **cryptologues** sont de nos jours presque tous des mathématiciens utilisant des fonctions mathématiques appelées ***algorithmes***.

3.3. Les algorithmes de cryptologie

Avant l'avènement des ordinateurs, la cryptographie traitait des algorithmes basés sur des lettres (ou caractères). Les différents algorithmes cryptographiques remplaçaient des caractères par d'autres ou transposaient les caractères. Les meilleurs systèmes faisaient les deux à la fois.
De nos jours, bien que beaucoup plus sophistiqué, le principe est resté le même. La différence majeure est que les algorithmes d'aujourd'hui manipulent les *bits* au lieu des caractères. Ce n'est finalement qu'un changement de taille d'alphabet : on passe de 26 éléments à 2 et rien de plus [13].

[5] Les mots en italique figurent dans le glossaire

3.3.1. Les algorithmes de substitution

Ce sont les méthodes les plus anciennes. Elles sont basées sur des techniques consistant à remplacer des données dans un message selon un ordre et une méthode déterminée.

Il y a quatre types de base de substitution : la substitution simple, homophonique, poly-alphabétique, simple par polygramme [2].

3.3.1.1. La substitution simple

Chaque caractère du texte en clair est remplacé par un caractère correspondant dans le texte chiffré.

L'exemple le plus connu est celui du **décalage de Jules César** [2] [53] où chaque caractère du texte clair est remplacé par celui qui se trouve 3 places plus loin dans l'alphabet modulo[6] 26.

Quelle que soit la lettre **t**, **c** vaudra **(t+4) mod 26**.

Ainsi, si t est un A (=0), c est un E (=4), donc A est remplacé par D, B par E, C par F, ..., X par A, Y par B, Z par C.

Par exemple le texte clair « JULES CESAR » devient « MXOHV FHVDU ».

Un autre algorithme par substitution simple est ROT13 [13]. Fréquemment utilisé par *UNIX* ROT13 n'est pas destiné à la sécurité mais pour cacher le texte pouvant être offensant, pour éviter trop tôt la solution d'un casse tête, etc. Chiffrer un fichier deux fois avec ROT13 redonne le fichier original.

3.3.1.2. La substitution homophonique

C'est le même principe que la substitution simple, sauf qu'à un caractère de texte en clair on fait correspondre plusieurs caractères dans le texte chiffré.

Par exemple, A correspond à 7, 15, 25 ou 56 ; P peut correspondre à 11, 13, 21 ou 42. Ainsi « PAPA » peut être chiffré 11,7,13,56 ou 21,15,21,15 ou 42,15,11,7, etc.

3.3.1.3. La substitution poly-alphabétique

Elle se compose de plusieurs algorithmes à substitution simple. Il peut y avoir autant d'algorithmes à substitution simples utilisés que de caractères composant le texte en clair. Celui qui est utilisé dépend de la position du caractère.

Prenons par exemple, le mot « CHAT » avec la table de substitution suivante :

		Alphabet en clair
		ABCDEFGHIJKLMNOPQRSTUVWXYZ
Phrase-clé	C	CDEFGHIJKLMNOPQRSTUVWXYZAB
	H	HIJKLMNOPQRSTUVWXYZABCDEFG
	A	ABCDEFGHIJKLMNOPQRSTUVWXYZ
	T	TUVWXYZABCDEFGHIJKLMNOPQRS

Alphabet de substitution

[6] L'arithmétique modulo est expliquée en annexes.

Le mot devient « EOAM ».

L'algorithme de chiffrement par substitution polyalphabétique est donc $c_i = t_i + k_i \bmod 26$.

L'algorithme de déchiffrement est $t_i = c_i - k_i \bmod 26$

3.3.1.4. La substitution simple par polygramme

Les caractères sont chiffrés par blocs. Par exemple « ABA » peut être chiffré par « RTQ » tandis que « ABB » est chiffré par « SLL » [13].

3.3.2. Les algorithmes de transposition

Ce procédé était utilisé par les allemands pendant la deuxième guerre mondiale sous le nom de **ADFGVC**. C'était un algorithme très compliqué pour l'époque mais il a été *cassé* par Georges PAINVIN, un *cryptanalyste* français. [13]

Le principe est de placer le texte clair horizontalement dans une grille de largeur fixe. On relève le texte chiffré verticalement.

Exemple :

Texte en clair : RENDEZ VOUS A PARIS DEMAIN MATIN

```
RENDEZVO
USAPARIS
DEMAINMA
TIN
```

Texte chiffré : RUDT ESEI DPA EAI ZRN VIM OSA

Si la sécurité d'un algorithme est basée sur le fait que celui-ci est secret (on parlera alors d'un algorithme restreint [13]), de tels algorithmes ne présentent plus qu'un intérêt historique car de nos jours ils sont inadéquats pour les besoins actuels de sécurité.
Pour la sécurité, les algorithmes modernes de chiffrement utilisent une clé. Cette clé peut prendre une des valeurs parmi un grand nombre de valeurs possibles. L'ensemble des valeurs possible d'une clé est appelé ***espace des clés*** [13].

Si l'on reprend l'exemple précédent en y insérant une clé, l'on obtient une transposition par clé.

Le procédé sera identique mais on associe au message à *crypter* une clé de cryptage en entête.
Le texte codé est formé en transmettant la colonne des lettres dans l'ordre alphabétique des lettres de la clé de cryptage.

Notre exemple devient :

Texte en clair : RENDEZ VOUS A PARIS DEMAIN MATIN

Clé de cryptage : CESAR

```
23514
CESAR
RENDE
ZVOUS
APARI
SDEMA
INMAT
IN
```

L'ordre alphabétique des lettres de la clé étant A C E R S, le texte chiffré devient :

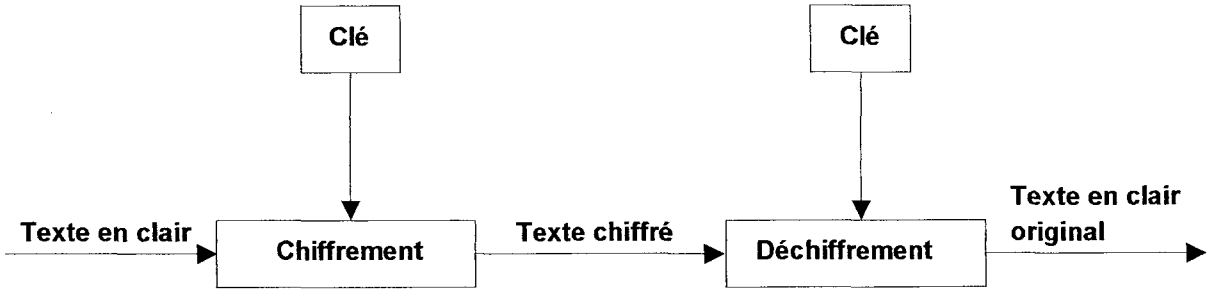
DURMA RZASII EVPDNN ESIAT NOAEM

Il existe deux types d'algorithmes à base de clé : à ***clé secrète*** ou à ***clé publique***.

3.3.3. Les algorithmes à clé secrète

Les algorithmes à clé secrète sont des algorithmes où la clé de chiffrement peut être calculée à partir de la clé de déchiffrement ou vice versa. Dans la plupart des cas, la clé de chiffrement et la clé de déchiffrement sont les mêmes. Pour de tels algorithmes, l'émetteur et le destinataire doivent se mettre d'accord sur une clé avant d'échanger des messages. Cette clé doit être gardée secrète. Si elle est dévoilée, alors n'importe qui peut chiffrer ou déchiffrer des messages.

Soit M, texte en clair, C le texte chiffré et k une clé appartenant à l'espace des clés K. Soit E, la fonction de chiffrement et D, la fonction de déchiffrement. La représentation graphique d'un système à clé secrète s'effectue comme suit :



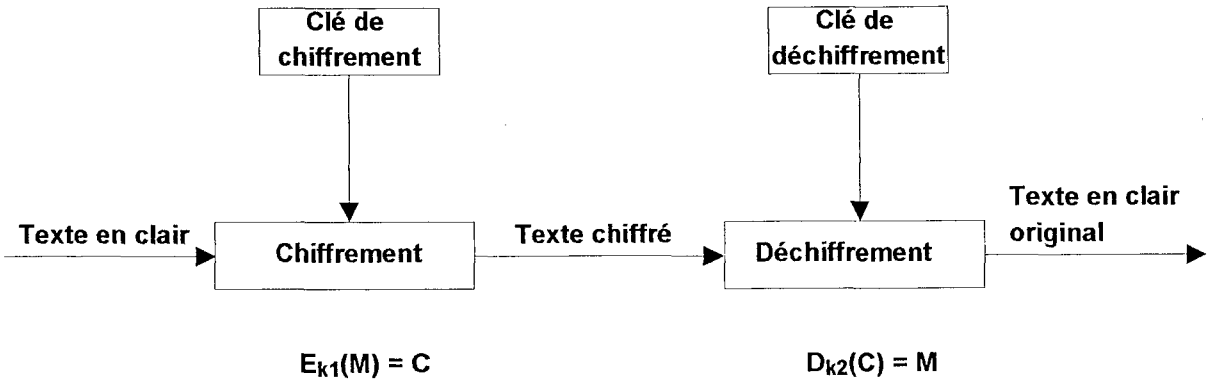
Si la clé de chiffrement est la même que la clé de déchiffrement, on a $D_k(E_k(M)) = M$ [13]

Un système de cryptage utilisant une même clé de déchiffrement et de chiffrement est appelé **cryptage symétrique**.

3.3.4. Les algorithmes à clé publique

Ils sont conçus de manière que la clé de chiffrement soit différente de la clé de déchiffrement. De plus, la clé de déchiffrement ne peut pas être calculée (du moins en un temps raisonnable) à partir de la clé de chiffrement. De tels algorithmes sont appelés « à clé publique » parce que la clé de chiffrement peut être rendue publique : n'importe qui peut utiliser la clé de chiffrement pour chiffrer un message, mais seul celui qui possède la clé de déchiffrement peut déchiffrer le message. Dans de tels systèmes, la clé de chiffrement est appelée ***clé publique*** et la clé de déchiffrement est appelée ***clé privée*** ou ***clé secrète***.

La figure ci-dessous illustre le chiffrement et le déchiffrement avec deux clés.



Si la clé de chiffrement est la même que la clé de déchiffrement, on a $D_{k2}(E_{k1}(M)) = M$ [4]

Un système de cryptage utilisant une clé de déchiffrement différente que la clé de chiffrement est appelé **cryptage asymétrique**.

3.4. Description des principaux algorithmes de cryptologie

Après avoir vu les grands principes des algorithmes de cryptologie, nous allons voir maintenant le détail des principaux algorithmes actuels.

3.4.1. DES

Créé en 1977 par la société américaine I.B.M. en langage *Fortran* [2], le **DES (Data Encryption Standard)** reste aujourd'hui l'algorithme le plus connu et le plus exploité. Utilisant à la fois les techniques de la **permutation** et de **substitution**, c'est un algorithme à **clé secrète**.

DES est un système de ***chiffrement par blocs***. Un bloc de 64 bits du texte clair entre par un côté de l'algorithme et un bloc de 64 bits de texte chiffré sort de l'autre côté.
Le chiffrement et le déchiffrement utilisent tous les deux le même algorithme. Le **DES** utilise une clé de chiffrement d'une longueur de **56 bits**[7]. Toutefois elle est exprimée comme un nombre de 64 bits, mais un bit sur huit sera ignoré.

[7] Une clé 56 bits (7 octets ou caractères) signifie 2 puissance 56 (plus de 72 millions de milliards) combinaisons de clés possibles.

On utilise souvent le **DES** pour chiffrer certaines grosses transactions bancaires et les codes personnels de cartes de crédit. Il est du plus utilisé par plusieurs ministères américains [59]. Il est de plus réputé pour sa vitesse d'exécution, ce qui le rend souvent utilisé pour chiffrer des messages longs [67].

L'algorithme se déroule 3 grandes parties :

Dans un premier temps on effectue une permutation **IP** (à l'aide de la matrice IP) sur chaque bloc de 64 bits. On a alors deux blocs de 32 bits, le premier appelé $\mathbf{L_0}$ et le second $\mathbf{R_0}$.

Puis, on effectue 16 rondes en appliquant la fonction récursive $\mathbf{R_i=L_{i-1}}$ **XOR** $\mathbf{f(R_{i-1},K_i)}$, où $\mathbf{K_i}$ sont des clés dérivées de la clé **K** et **f** est la fonction décrite en détail plus loin.

Nous connaissons donc les $\mathbf{L_{i-1}}$ et $\mathbf{R_{i-1}}$ définis à l'étape **i-1**, et les 16 matrices permettant de calculer les 16 clés dérivées $\mathbf{K_i}$ à partir de **K** (matrices).
La dernière étape consiste à appliquer la fonction inverse de **IP** à $\mathbf{R_{16}L_{16}}$ afin de chiffrer le texte (matrices de IP inverse).

Etude de **f** :
Le premier bloc $\mathbf{R_{i-1}}$ est augmenté de 32 bits à 48 bits, à l'aide d'une permutation **E** (matrice de E) où certains blocs sont dupliqués. On a alors $\mathbf{E(R_{i-1})}$.
On effectue l'opération $\mathbf{E(R_{i-1})}$ **XOR** $\mathbf{K_i}$ puis on découpe le résultat obtenu (c'est-à-dire la chaîne de 48 bits) en 8 sous-chaînes de 6 bits. $\mathbf{K_i}$ est une des 16 clés dérivées obtenue à partir de **k** et des 16 tables associées (tables).
Pour résumer $\mathbf{B_i=E(R_{i-1})}$ **XOR** $\mathbf{K_i}$ avec $\mathbf{B=B_1B_2...B_8}$ quel que soit i.
On affecte un nombre entier compris entre 1 et 8 à chaque $\mathbf{B_j}$ à l'aide des tableaux $\mathbf{S_j}$ (tableaux).
Soit $\mathbf{B_j=c_1c_2c_3c_4c_5c_6}$ (où $\mathbf{c_k}$ est le $k^{ème}$ bit), le nombre constitué des bits $\mathbf{c_1c_6}$ indiquera la ligne et le nombre constitué des bits $\mathbf{c_2c_3c_4c_5}$ indiquera la colonne du tableau $\mathbf{S_j}$.
$\mathbf{S_j}$ est donc un tableau de 4 lignes et 16 colonnes.
La chaîne ainsi obtenue est réordonnée suivant une dernière permutation fixée **P** 'matrice de P).

Les étapes avec les matrices, tables et tableaux sont reprises en annexes.

Le 19 janvier 1997, le DES a été *cassé* en 22 heures et 15 minutes.

Le challenge DES-III de cassage de clé organisé par RSA inc [67], a été remporté par Distributed [63] en 22 h 15 mn. Le message crypté avec l'algorithme DES utilisant une clé de 56 bits était : « See you in Rome (second AES conference, March 22-23, 1999) ». La vitesse de recherche de clés était de l'ordre de 200 Gclés/sec. C'est la machine Deep Crack[8] de l'EFF (Electronic Frontier Fondation) [56], qui collaborait au challenge, qui a trouvé la clé. C'était déjà elle qui avait craqué seule le challenge DES-II en 56 heures en juillet 1998.

3.4.2. RSA

L'algorithme **RSA** est le plus populaire des algorithmes à ***clé publique***. Il est aussi le plus facile à réaliser. Baptisé d'après le nom de ces inventeurs, **Ron RIVEST**, **Adi SHAMIR** et **Léonard ADLEMAN**, qui construisirent pour la première fois l'algorithme en 1977, on l'appelle aussi parfois [2] [4] le **MIT** car il a été développé au Massachusetts Institute Technology [49].

La sécurité du système repose sur l'impossibilité d'effectuer la factorisation d'un grand nombre [2] [4] de quelques centaines de chiffres en un temps raisonnable. Les clés publiques et privées sont des fonctions d'une paire de grands *nombres premiers* (nombre de 100 à 200 chiffres ou plus encore) [13].

[8] Photo en annexes.

Retrouver le texte en clair à partir d'une des clés est équivalent à la factorisation du produit des deux *nombres premiers*.

Pour engendrer les deux clés, l'utilisateur choisi deux grands nombres premiers, **p** et **q**. Il possède alors une clé publique constituée du produit **n** de deux *nombres premiers* **p** et **q** (**n = p x q**).

p et q doivent rester secret

Il choisit ensuite une clé de chiffrement aléatoire **e** tel que **e** et **(p - 1) x (q - 1)** soient premiers entre eux.
La *clé secrète* est l'inverse **d** de **e** : $d = e^{-1} \bmod ((p - 1) \times (q - 1))$.

Pour chiffrer un message **c** représenté par un nombre modulo **n**, on élève **c** à la puissance **e** modulo **n**. On obtient alors **c'**, le message chiffré. Pour retrouver **c** à partir de **c'**, on élève **c'** à la puissance **d** modulo **n**.

Ainsi, le message chiffré **c** sera constitué de manière similaire de bloc c_i d'à peu près la même longueur. La formule de chiffrement est simplement [13] :

$$c_i = m_i^e \bmod n$$

Pour déchiffrer un message, chaque bloc c_i est calculé :

$$m_i = c_i^d \bmod n$$

Un exemple de chiffrement RSA est en annexes.

Personne n'a encore à ce jour pu *casser* RSA. Le problème est que **n** étant public, le *cryptanalyste* pour trouver **p** et **q** afin de calculer **e** doit factoriser un grand nombre en deux facteurs premiers.
De ce fait, plus la clé est longue, plus le nombre de possibilités sera grand.
On a calculé qu'avec une clé de 664 bits, en faisant l'hypothèse qu'un ordinateur peut effectuer un million de d'étapes de factorisations par seconde et qu'un réseau d'un million d'ordinateurs dédié à cette tâche, il faudra environ 4000 ans pour factoriser le nombre. Avec une clé de 1024 bits, le même réseau d'ordinateurs prendra 10^{10} années.
Pourtant, certains considèrent qu'une clé de 1024 bits restera sûre pour une dizaine d'année et envisagent l'utilisation de clé à 2048 bits.

L'inconvénient du RSA est qu'il est lent. En logiciel, le DES est environ 100 fois plus rapide que le RSA. C'est pourquoi la plupart des systèmes utilisent le RSA pour l'échange de clés DES et utilisent ensuite DES pour chiffrer le reste.

3.4.3. IDEA

IDEA (de International Data Encryption Standard) est un algorithme de chiffrement classique conçu par Xueja LAI et James MASSEY. Dans sa première version en 1990, il s'appelait PES (Proposed Encryption Standards). Puis après quelques améliorations, il fut appelé IPES (Improved Proposed Encryption Standards), pour enfin prendre son nom actuel en 1992. Certains disent qu'il s'agit du meilleur et du plus sûr des algorithmes disponibles publiquement à ce jour [13].
Il agit sur des **blocs** de texte clair de **64 bits** à l'aide d'une **clé** de **128 bits**. Il repose uniquement sur trois opérations algébriques : un **XOR**[9], une **addition modulo 2^16**, et une **multiplication modulo 2^16 + 1**.

[9] XOR est le OU EXCLUSIF

Le bloc de texte clair de 64 bits sera divisé en 4 blocs de 16 bits ; et la clé, elle, sera divisée en 6 blocs de 16 bits. L'algorithme effectuera 8 rondes combinant à l'aide de nos trois opérations les 4 premiers blocs aux 6 autres. Soient *X1*, *X2*, *X3* et *X4* nos 4 blocs de texte clair qui seront nos 4 entrées, *Z1*, *Z2*,..., *Z6* les 6 blocs de notre clé. A la fin, il suffira de réassembler les 4 sous blocs chiffrés.

IDEA est un algorithme rapide. Sa version logicielle est presque aussi rapide que le DES [13].

Les séquences d'événements de l'algorithme sont décrites en annexes.

3.4.4. D'autres algorithmes

Nous allons dans ce paragraphe énumérer quelques-uns uns des nombreux autres algorithmes existants. Le choix de ces algorithmes a été fait en fonction de leur utilisation et popularité.

3.4.4.1. RC4

Algorithme de chiffrement en continu à **clé privée** de longueur variable développé par Ron Rivest pour RSA Data Security en 1987.

RSA Data Security prétend que RC4 est dix fois plus rapide que DES.

Il chiffre des blocs de 64 bits avec une clé de 40 bits [13]. Il existe aussi une version 128 bits utilisée exclusivement aux Etats-Unis [48].

Il utilise une table $\mathbf{S_i}$, permutations de 255 octets.

Algorithme :

- $i = (i + 1) \bmod 256$
- $j = (j + S_i) \bmod 256$
- Echanger S_i et S_j
- $t = (S_i + S_j) \bmod 256$
- $K = S_t$

3.4.4.2. MD5

Après un traitement initial, **MD5** manipule le texte d'entrée par blocs de **512 bits** divisés en **16 sous-blocs de 32 bits**. La sortie de l'algorithme est un ensemble de **4 blocs de 32 bits** qui, joints ensemble, forment une seule empreinte de **128 bits** [13].

MD5 est utilisé pour l'authentification et la gestion des clés, dans *PGP* [75]. Une description de l'algorithme se situe en annexes.

3.4.4.3. El gamal

ElGamal est un procédé complexe, dont la résistance à la cryptanalyse est mathématiquement sure.

Son défaut principal est sa lenteur d'exécution qui ne permet pas d'utilisation directe et concrète dans la vie quotidienne. Par contre le principe de signature qui en découle est facile a mettre en oeuvre et couramment utilise.
ElGamal n'est pas breveté. La société PKP considérait que cet algorithme était couvert par le Brevet du système de Diffie-Hellman mais celui-ci a expire le 29 avril 1997.
ElGamal est désormais le premier algorithme cryptographique à **clé publique** qui ne soit pas couvert par un brevet aux Etats-Unis.

Pour engendrer une paire de clés, il faut choisir d'abord un *nombre premier* **p** et deux nombres aléatoire **g** et **x** tels que **q** et **x** soient tous deux **inférieurs** à **p**. Ensuite on calcul $\boxed{y = g^x \bmod p}$
La clé publique est faite de **y**, **g** et **p**. Les valeurs de **g** et **p** peuvent être toutes deux partagées par un groupe d'utilisateurs. La *clé privée* (ou *secrète*) est **x**.

Chiffrement ElGamal : [13]

CLE PUBLIQUE
p premier
$g < p$
$y = g^x \bmod p$

CLE PRIVEE
$x < p$

CHIFFREMENT
k choisi aléatoirement et premier avec p - 1
a (texte chiffré) $= g^k \bmod p$
b (texte chiffré) $= y^k M \bmod p$ (M est le texte en clair)

DECHIFFREMENT
M (texte en clair) $= b/y^a \bmod p$

3.4.4.4. Diffie-Hellman

Diffie-Helman est le premier algorithme à clé publique qui fut inventé. Il peut être utilisé pour la distribution de clé mais pas pour *crypter* ou *décrypter* des messages [13].

Inventé en 1976 par Diffie et Hellman, ce protocole permet à deux tiers de générer un secret partagé sans avoir aucune information préalable l'un sur l'autre. Il est basé sur la cryptologie à clé publique (dont il est d'ailleurs à l'origine), car il fait intervenir des valeurs publiques et des valeurs privées. Sa sécurité dépend de la difficulté de calculer des logarithmes discrets sur un corps fini. Le secret généré à l'aide de cet algorithme peut ensuite être utilisé pour dériver une ou plusieurs clés (clé secrète, *clé de chiffrement de clés*,...).
Voici le déroulement de l'algorithme :

1. *Alice* et *Bob* se mettent d'accord sur un grand entier *n* tel que *(n-1) / 2* soit premier et sur un entier *g* primitif par rapport à *n*. Ces deux entiers sont publics.
2. Alice choisit de manière aléatoire un grand nombre entier *a*, qu'elle garde secret, et calcule sa valeur publique, $A = g^a \bmod n$. Bob fait de même et génère *b* et $B = g^b \bmod n$.
3. Alice envoie *A* à Bob ; Bob envoie *B* à Alice.
4. Alice calcule $K_{AB} = B^a \bmod n$; Bob calcule $K_{BA} = A^b \bmod n$. $K_{AB} = K_{BA} = g^{ab} \bmod n$ est le secret partagé par Alice et Bob.

Une personne qui écoute la communication connaît *g, n, A=g^a mod n* et *B=g^b mod n*, ce qui ne lui permet pas de calculer g^{ab} *mod n* : il lui faudrait pour cela calculer le logarithme de *A* ou *B* pour retrouver *a* ou *b*.

3.4.4.5. Blowfish

Blowfish est un algorithme crée par Bruce Schneier; président de Counterpane Systems [47], société américaine de consultation dans la sécurité informatique et cryptographie [76].

Il chiffre des blocs de 64 bits en 16 itérations. Il utilise une clé à longueur variable de 448 bits minimum.

L'algorithme fonctionne en deux parties : une partie pour étendre la clé jusqu'à 4168 bits et l'autre pour le cryptage des données.
Le chiffrement s'effectue en 16 occurrences. A chaque tour on permute et on substitue la clé. Toutes les opérations sont des **XOR** additionnés sur un bloc de 32 bits.
Blowfish utilise un grand nombre de sous-clés. Ces clés doivent être traitées avant le cryptage ou le décryptage.

Les étapes du blowfish sont exposées en annexes.

3.5. Les domaines d'utilisation des algorithmes

3.5.1. Les protocoles

Il s'agit de protocoles permettant de négocier interactivement des algorithmes de chiffrement. Le plus souvent, c'est RC4 qui est choisi, et notamment RC4 40 bits dans les versions exportables de Netscape (*cf chapitre sur la législation française en matière de cryptologie*), mais ce n'est qu'une possibilité. Par exemple, aux USA, il est possible d'utiliser RC4 128 bits. Ces algorithmes sont à *clé symétrique*, à usage unique.

3.5.1.1. SSL

La spécification du **protocole SSL** comprend essentiellement deux parties : le protocole "Poignée de main" (Handshake Protocol) [108], qui établit la connexion en effectuant une authentification initiale avec transfert des clés publiques, et le protocole **Transfert des données** (Record Protocol) qui, une fois la connexion faite, sert à transférer les messages et les données en utilisant divers algorithmes d'authentification et d'encryptage. En raison de l'interdiction par la loi américaine d'exporter la cryptographie en dehors des Etats-Unis, les versions exportables des navigateurs et serveurs W3 (World Wide Web) de Netscape et de Microsoft utilisent les clés privées **RC4** (Rivest's Code #4) de 40 bits de longueur avec les clés publiques de 512 bits, alors que les versions domestiques (Etats-Unis et Canada) utilisent les clés privées à 128 bits de longueur. Les deux versions utilisent l'algorithme RSA (Rivest-Shamir-Adleman) pour l'encryptage à clé publique.
Parce que SSL s'insère entre HTTP et *TCP/IP*, le même serveur W3 peut facilement différencier les requêtes sécuritaires des requêtes normales et, en conséquence, les traiter différemment.
Les requêtes pour les pages W3 sécurisées avec SSL commencent par « **https://** » et non par « **http://** » comme dans le cas de HTTP standard. Dans Netscape Navigator, lorsque SSL est activé, la petite clé dans le coin inférieur gauche s'affiche pleine, sans brisure.
Netscape Communications rend gratuite la distribution du code source de SSL à son site [107]. La version 3.0 de SSL offre une large gamme de fonctions cryptographiques, bien que seulement une partie de celles-ci soit supportée par les clients et serveurs W3. Il est plus facile d'implémenter SSL que S-HTTP dans une application TCP/IP existante.

3.5.1.2. S-HTTP

Développé par Enterprise Integration Technology (EIT, Menlo Park, CA), **S-HTTP** utilise une version modifiée de HTTP qui procure au client et au serveur W3 (World Wide Web) l'habileté de négocier l'authenticité, la **confidentialité** et l'***intégrité*** des **transactions**. L'implémentation de S-HTTP se trouve au niveau de la couche application du *modèle ISO/OSI* (International Standards Organization / Open Systems Interconnection). De nouveaux en-têtes sont ajoutés au message HTTP original, spécifiant entre autres les exigences d'encryptage (la réponse doit être encryptée et signée, par exemple), l'algorithme cryptographique avec les paramètres supportés et l'ensemble des consignes à propos des clés et certificats. Le nouveau message est encrypté/signé et *encapsulé* dans le message S-HTTP qui se voit ajouter des en-têtes décrivant de quelle façon le récepteur du message protégé doit s'y prendre pour restituer le message original.
Les serveurs W3 reconnaissent les URL (Uniform Resource Locator) qui exigent S-HTTP lorsque ceux-ci débutent par « **shttp://** » au lieu de « **http://** », ou se terminent par « .html » plutôt que par « .html ». S-HTTP offre une large gamme de fonctions cryptographiques. Plusieurs serveurs W3 supportent S-HTTP, dont les serveurs W3 de NCSA (National Center for Supercomputing Applications), Apache, CERN, Spyglass et IBM.

3.5.1.3. SET

SET (Secure Electronic Transactions) a été développé par MasterCard, Visa, American Express, Microsoft, IBM, Netscape, et Teresa Systems, c'est à dire par l'ensemble des acteurs du marché. Le protocole SET se base sur un certificat numérique utilisant le cryptage **RSA** en substitution du numéro de la carte bancaire, de sorte que ce dernier ne transite pas sur le réseau.
Au départ, le client envoie à Visa ou à Mastercard (à l'aide d'un programme annexe (plug-in) se greffant sur son navigateur) un fichier généré à partir de ses coordonnées bancaires. L'organisme financier lui envoie en retour une clé (RSA) qui servira au client de moyen d'authentification auprès d'un commerçant. Il peut vérifier la validité de cette clé auprès de la banque du client. Netscape a intégré SET à son navigateur et la plupart des éditeurs de solutions de paiement électronique sur le marché prévoient également de l'implémenter.

3.5.1.4. SSH

Secure Shell (**SSH**) est une version sécurisée des programmes usuels de connexion à distance sur *UNIX* : rlogin, rsh et rcp. Leurs équivalents sont slogin, ssh et scp, qui leur sont parfaitement compatibles au niveau utilisateur (transparence), mais font de l'authentification et du chiffrement par en dessous.

3.5.1.5. JEPI

Les protocoles précédants ont l'avantage d'être universels. Par contre les solutions propriétaires sont incompatibles entre elles. C'est pour cette raison qu'est né le **Jepi** (Joint Electronic Payment Initiative) qui assure le lien entre différents protocoles ou logiciels de paiement.

3.5.2. Les logiciels

Il existe de nombreux logiciels sur le marché. Si certains sont très connus, tel PGP, et d'autres essayent de le devenir, ils sont pour la plupart des programmes simples, uniquement basés sur l'algorithme qu'il utilise, et non sur la sophistication de l'interface (beaucoup tournent sous *DOS*).

Il existe en fait une multitude de logiciels en *freeware* que l'on peut très facilement se procurer en les téléchargeant depuis l'internet.
Toutefois, les logiciels commerciaux se heurtent à la réglementation française, qui interdit l'utilisation d'une clé de plus de 40 bits (cf chapitre législation française en matière de cryptologie). Les Etats-Unis, notamment, interdisent toute commercialisation vers en dehors de leur territoire et du Canada.

3.5.2.1. PGP

PGP est l'abréviation de "**Pretty Good Privacy**". C'est un logiciel gratuit développé par Philip Zimmermann, un informaticien américain. Ayant diffusé son logiciel sur Internet, il a été poursuivi un temps aux USA pour trafic d'armes (la cryptographie est considérée par les autorités comme une arme non exportable). Selon une estimation faite en 1997 par la société PGP Inc. [77], plus de 4 millions de copies du logiciel seraient en circulation dans 50 pays du globe. PGP a été traduit jusqu'ici en 25 langues.

PGP fonctionne sur différentes plates formes comme Windows, MsDos ou Unix. Il utilise les algorithmes **IDEA** pour le chiffrement, **RSA** et **MD5** pour l'authentification et la gestion des clés. Les messages sont donc chiffrés à l'aide d'un système à clé unique (*symétrique*), mais cette clé, insérée dans le message, est chiffrée à l'aide d'un système à *clé publique* (**RSA**).
Des versions existent destinées à être intégrées dans des clients E- Mail et le téléphone (PGPfone, PGPTalk).

PGP est un logiciel de chiffrement dont les sources sont intégralement rendues publiques [90]. Il est distribué depuis 1991, et le temps qui passe confirme toujours plus la robustesse de l'algorithme. La seule chose à craindre réside dans les progrès en mathématiques, pour optimiser la factorisation des grands nombres [80]. De très gros progrès ont été faits récemment, mais ils nécessitent des moyens uniquement à la portée des Etats. Malgré cela la parade est simple : il suffit d'augmenter la taille de la clé.
Il est actuellement conseillé de générer une paire de clés de 3072 bits chacune pour PGP 5.x ou 6.x et de 2048 bits pour PGP 2.6x. Le mot de passe protégeant la *clé secrète* doit être de 20 à 25 caractères minimums (un mot de passe de 5 à 6 caractères est tout simplement inutile : quiconque aura accès à la clé secrète pourra craquer ce mot de passe !). Dans l'idéal, pas de mot, de noms communs ou de noms propres, ni de dates ou de nombres ayant une signification quelconque. Dans la pratique, une phrase dont on se rappellerait.

La loi interdit formellement d'importer un logiciel de cryptographie à partir d'un pays extérieur à la CE, sans une autorisation du Premier Ministre [117]. Mais l'importation à partir de l'Allemagne, Italie, Finlande, des Pays-Bas, de la Suède et du Royaume-Uni libre [94 à 101].

PGP est interdit en France. Cependant depuis la décision du CISI (Conseil Interministériel pour la Société de l'Information) du 19 janvier 1999 et le discours du Premier Ministre Lionel Jospin qui l'a suivi [120], la libéralisation totale de la cryptologie est en marche. Les logiciels de cryptographie dont la longueur de clé n'excède pas 128 bits seront libres d'utilisation.

Bien que PGP soit un programme gratuit, il utilise les algorithmes **RSA** et **IDEA** qui sont protégés.
RSA est protégé aux USA, et y est distribué sous la forme de la bibliothèque RSAREF. La version de PGP qui utilise cette bibliothèque est actuellement la 6.x du MIT (Massachusetts Institute Technology) [49], et ne peut être exportée des USA (mais les versions exportées peuvent être utilisées). Hors des USA, RSA a été complètement réécrit, et cette autre version appelée MPILIB, non soumise à une licence, est intégrée dans la version 2.6.3i de PGP [87], qui ne peut être utilisée aux USA.
IDEA est protégé dans certains pays d'Europe, dont la France. Les droits sont détenus par Assomme Siestes A.G., en Suisse. Néanmoins l'utilisation non commerciale de IDEA est libre.

3.5.2.2. *Security Box*

Logiciel à *clé secrète* **Security Box** est un logiciel français diffusé par la Société de Services en Ingénierie Informatique (SIS) MIS (Méthode et Solution Informatique) crée en 1988 et située à Versailles. Elle est aussi implantée en Ile de France, Rhône-Alpes et Bretagne.

Le logiciel permet de crypter un ou une liste de fichiers et/ou de répertoires.

Son prix est de 1900.00 F ou de 4500.00 F hors taxes, selon la licence choisie.

Une version d'évaluation gratuite est disponible pendant 30 jours et téléchargeable sous [102].

3.5.2.3. *CRYPTMAIL*

Le logiciel de chiffrement **Cryptmail** est destiné à pallier au manque de confidentialité de la messagerie électronique. Crée et distribué par la société française Topteck, c'est un logiciel dédié à Microsoft Exchange. Il permet de chiffrer, de manière transparente pour l'utilisateur, tout type de données transmises avec Exchange, qu'il s'agisse de messages texte ou de documents attachés.

Deux algorithmes de chiffrement : **DES** et **IDEA**. Pour le chiffrement, Cryptmail fait appel à deux algorithmes différents. Pour une utilisation dans le domaine financier, c'est le **DES** (Data Encrytpion Standard) qui a été choisi, avec une clé de 56 bits. Dans les autres domaines, est employé l'algorithme IDEA, avec une clé de 128 bits. Les clés de chiffrement peuvent être stockées en dehors de la machine, sur disquettes ou même sur cartes à puce. Pour ces deux algorithmes, Cryptmail a reçu l'agrément du SCSSI (Service central de la sécurité des systèmes d'information) [124].
Sur demande, la société Topteck peut inclure dans la solution d'autres algorithmes, logiciels ou matériels, sous réserve que le client ait obtenu au préalable l'agrément correspondant auprès du SCSSI (*cf chapitre sur la législation*).
Cryptmail est disponible sous Windows 95, 3.1x et NT, à partir de 15 000 francs (5 licences). Un tarif dégressif est appliqué jusqu'à 50 licences ; à partir de 100 utilisateurs, le tarif est négocié avec le client.

3.5.2.4. *Les logiciels freeware et shareware*

Les codes sources des algorithmes étant édités [9] [13], un programmeur pourra créer son propre programme. Beaucoup s'y essayent et diffusent gratuitement LEUR algorithme sur internet. Presque tous ces programmes utilisent une *clé secrète*, cryptent le fichier dans un nouveau fichier et tournent sous *DOS*.

Il conviendra de vérifier que le programme téléchargé respecte bien la loi française.

3.6. La législation française en matière de cryptologie

3.6.1. Problématique

La France présente la particularité d'avoir une des réglementations les plus restrictives du monde quant aux droits aux citoyens de protéger des secrets.
Héritée en droite ligne de la guerre froide et d'une époque ou la cryptologie était une discipline réservée aux militaires, la loi française privilégie la sécurité nationale ou une trop grande sécurité interdit tout contrôle.

Dès 1939, le chiffrement, qui n'avait alors rien de numérique, était intégré dans la liste des "matériels de guerre, armes et munitions". Ce n'est que depuis la loi du 29 décembre 1990 que la cryptologie dispose d'un régime sensiblement plus ouvert. En effet, le régime juridique français de la cryptologie a pour caractéristique essentielle de procéder à une distinction entre les différentes fonctions assurées par les moyens de chiffrement, et non entre leur puissance. Cette démarche, qui tente, parfois avec difficulté, de faire la part entre le fait de garantir l'authentification d'un message, d'assurer son intégrité, ou de préserver sa confidentialité, apparaît particulièrement éloignée du système américain. Aux Etats-Unis, le débat juridique, mais aussi technique et économique, se situe au niveau de la puissance des algorithmes

3.6.2. La loi de 1990

La fourniture, l'utilisation, l'exportation, l'importation de systèmes de chiffrement sont soumis à déclaration pour la simple authentification, et à l'autorisation du Premier Ministre pour la confidentialité. En pratique, il n'y a pas de différence entre les deux cas. L'autorisation est très rarement accordée. Les critères ne sont pas connus, et sont vraisemblablement conditionnés par la facilité de décryptage ou le dépôt des clés.

L'importation , la fourniture ou l'utilisation de moyens ou de prestations de cryptologie provenant de pays n'appartenant à la Communauté Européenne est interdite et sévèrement punie.

Nul n'a le droit de fournir, utiliser ou exporter des moyens ou des prestations de cryptologie sans autorisation préalable du SCSSI (Service Central de la Sécurité des Systèmes d'Information) [124]. *(Loi no. 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications)* [112].

Les **peines prévues** sont *(art. 15 du décret 92-1358 du 28 décembre 1992)* [115]:

- **fourniture** ou **utilisation** sans autorisation d'un **moyen** de cryptologie :
  amende correspondant aux contraventions de 5e classe
  (c'est-à-dire - *art. 131-13 du nouveau Code pénal* - 10 000 F, 20 000 F en cas de récidive)
- **fourniture** sans autorisation d'une **prestation** de cryptologie, ou
- **exportation** sans autorisation :
  amende de 6 000 à 300 000 F et / ou emprisonnement de 1 à 3 mois.

3.6.3. La loi de 1996

La loi du 26 Juillet 1996 modifie la loi de 1990. Elle introduit à l'article 17 la notion d'organisme agréé (surnommé ***Tiers de Confiance***), qui aurait la charge de gérer les conventions secrètes, c'est-à-dire, a priori, les clés de chiffrement. [115]

Le **Tiers de confiance**, neutre, est désigné par les parties comme témoin des transactions électroniques. Le tiers de confiance, en sa qualité d'intermédiaire, protège l'émetteur contre la mauvaise foi du récepteur Ce dernier ne peut nier la réception effective du message, et réciproquement. Son rôle est d'assurer la sécurité des transactions sans ingérence dans le contenu et de fournir aux parties des preuves irréfutables en cas de contentieux. Le tiers de confiance remet les *clés privées* à la justice en cas d'enquête pénale. Il assure :

L'identification certaine des opérateurs (émetteur et récepteur).
L'intégrité du message.
La confidentialité des opérations.
La non-répudiation des opérations.
L'horodatage des opérations (date et heure).

Le décret d'application établit la dispense de formalité pour les opérations portant sur des procédés de cryptage dont les conditions d'utilisation sont telles qu'elles ne sont en aucun cas susceptibles de porter atteinte à la sécurité intérieure ou extérieure de la France.
Dans tous les autres cas, la fourniture, l'importation ou l'exportation sans autorisation préalable de l'Etat demeurent illégales. Les peines sont nettement renforcées, elles passent de 10 000 F d'amende à six mois de prison et 200 000 F d'amende. On comprend alors que le télépaiement sur Internet ait tant de mal à se développer en France, car les clients et les banques ont besoin de garantir la confidentialité

3.6.4. La loi de 1998

Deux décrets du 24 février 1998 concernent, d'une part, la procédure de déclaration et d'autorisation des moyens de cryptologie et, d'autre part, l'agrément et le mode de fonctionnement des organismes du **Tiers de confiance**, chargés de gérer les "conventions secrètes", c'est-à-dire les clés de chiffrement. La libéralisation de l'utilisation de ces outils s'est faite de plus en plus pressante au fur et à mesure du développement des réseaux ouverts dans leur ensemble, et d'Internet en particulier.

Devant ces revendications, un troisième décret paru le du 23 mars 1998, a défini la liberté d'utilisation de la cryptologie dans un but de confidentialité si la clé de chiffrement utilisée ne dépasse pas 40 bits. Ce plafond a suscité (et suscite encore) de vives réactions dans les milieux concernés, au motif qu'il serait notoirement insuffisant pour permettre aux entreprises françaises d'être compétitives sur les réseaux.

3.6.5. L'abrogation de la loi ?

Le **19 janvier 1999**, le Premier Ministre, Monsieur Lionel Jospin, a prononcé un discours visant l'abrogation de la loi anti-cryptographique française [120].
Estimant la loi en cours inadaptée, le Gouvernement a retenu les orientations suivantes :

- offrir une liberté complète en matière de cryptologie
- supprimer le caractère obligatoire du recours au *tiers de confiance* pour le dépôt des clés de chiffrement
- compléter le dispositif juridique actuel par l'instauration d'obligations, assorties de sanctions pénales, concernant la remise aux autorités judiciaires, lorsque celles-ci la demandent, de la transcription en clair des documents chiffrés.

Cette loi pouvant prendre plusieurs mois, dans l'attente, le Gouvernement a décidé de **relever le seuil de la cryptologie de 40 bits à 128 bits**, niveau considéré par les experts comme assurant durablement une très grande sécurité.

3.7. Conclusion

Entre l'évolution permanente de la puissance des ordinateurs et la croissance des moyens modernes de communications, la sécurité informatique risque d'être un sujet de plus en plus d'actualité.

Si de nos jours les moyens de sécurité sont fiables, qu'en sera-t-il demain ? Qui aurait pensé il y a 20 ans que le DES pouvait être cassé en moins de 24 heures ?
La puissance grandissante des ordinateurs accentuera-t-elle la course poursuite entre les concepteurs de sécurité, ceux qui créent des algorithmes de cryptologie, des logiciels ou des protocoles de sécurité et les *cryptanalyste* ?

La sécurité actuelle repose sur la longueur de la clé de cryptage. Pour remédier au piratage, faudra-t-il sans cesse augmenter la taille des clés ? Ce problème n'est pas prêt d'être résolu car les Etats n'ont pas la même perception de la nécessité d'empêcher les citoyens de dissimuler leurs secrets à leur guise, dès lors que ces secrets ne sont pas de nature criminelle.

4. Glossaire

Algorithme (cryptologique, de cryptographie, de cryptologie, de cryptage, de chiffrement)

Procédé permettant, avec l'aide d'une *clé*, de *chiffrer* et de *déchiffrer* des messages ou des documents. Un bon algorithme n'a pas besoin d'être secret pour être sûr. En effet, il faut toujours supposer que l'ennemi dispose d'un exemplaire du matériel ou du logiciel qui le réalise ; dans ces conditions, il peut l'analyser (le décompiler, par exemple). Le secret du chiffre ne doit dépendre que du secret de la clé.

Alice, Bob et les autres

Alice est le nom donné dans la littérature cryptologique à la personne qui prend l'initiative d'une communication. Son interlocuteur s'appelle **Bob**. **Eve** est une espionne qui cherche à lire le message. **Mallet** est un "ennemi intervenant actif" qui cherche à falsifier le message.
Si vous lisez les publications spécialisées, vous rencontrerez donc très souvent des phrases du genre : "Alice veut envoyer un message à Bob". Cela permet d'utiliser ensuite simplement "A" et "B" dans les formules, tout en restant facilement compris.

Bibliographie courante

Bibliographie recensant des documents au fur et a mesure de leur publication.

Bibliographie rétrospective

Bibliographie recensant des documents publiés durant une période révolue.

Bit

Binary digIT. Le plus petit élément d'information en système binaire. Un **bit** peut donc valoir un **0** ou un **1**. Ne pas confondre avec l'anglais byte qui signifie *octet*.

Bruit

Le bruit correspond à la proportion de documents non pertinents retrouvés.

Casser un algorithme de cryptologie, une clé

Un algorithme est cassé dès lors que la clé de chiffrement qu'il utilise a été trouvée alors que l'on ne la connaissait pas. Une clé qui a été cassée implique que l'algorithme n'est pas assez puissant.

Chiffrement, 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"***, de même que les substantifs ***"cryptage"*** et ***"encryptage"*** sont des anglicismes que les amoureux de la langue française éviteront).

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 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***.

Clé de chiffrement

Clé utilisée exclusivement pour *chiffrer* d'autres *clés*, afin de les faire parvenir à un interlocuteur. Une ***clé de chiffrement*** a généralement une durée de vie assez longue, par opposition aux clés qu'elle sert à *chiffrer*.

Clé de session

Une **clé de session** est une ***clé secrète*** qui sert à chiffrer une communication (éventuellement dans les deux sens, et / ou entre plus de deux participants). Normalement, on **change** de clé de session **à chaque transmission**. Elle est le plus souvent créée de manière **aléatoire** ; il faut donc un procédé pour la faire connaître par tous les participants. Ce procédé utilise souvent une *clé publique*.

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.

Cryptage, crypter

Termes dérivés de l'anglais **to encrypt** et souvent employés incorrectement à la place de *chiffrement* et *chiffrer*. En toute rigueur, ces termes n'existent pas dans la langue française. Si le ***cryptage*** existait, il pourrait être défini comme l'inverse du *décryptage*, c'est-à-dire comme l'action consistant à obtenir un *texte chiffré* à partir d'un *texte en clair* sans connaître la *clé*. Un exemple concret pourrait être de signer un texte choisi en reproduisant un chiffrement avec la *clé privée* de la victime. Mais on préfère parler dans ce cas de contrefaçon.

Cryptanalyse ou analyse cryptographique

Science qui étudie la sécurité des procédés cryptographiques pour tenter de trouver des faiblesses et pouvoir en particulier effectuer un ***décryptement*** avec succès.
"Analyse d'un système cryptographique, et/ou de ses entrées et sorties, pour en déduire des variables confidentielles et/ou des données sensibles (y compris un *texte en clair*)." [ISO 7498-2]

Cryptogramme

Aussi appelé *texte chiffré*. Données obtenues par application d'un algorithme de chiffrement. Le contenu sémantique de ces données n'est pas compréhensible.

Cryptographie

Etude du *chiffrement* et du *déchiffrement*, ainsi que des procédés permettant d'assurer l'intégrité, l'authentification,...
"Discipline incluant les principes, moyens et méthodes de transformation des données, dans le but de cacher leur contenu, d'empêcher que leur modification passe inaperçue et/ou d'empêcher leur utilisation non autorisée." [ISO 7498-2]

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, ***Bob***, qui déchiffre. L'opération ou son résultat s'appelle un **déchiffrement**.
Décrypter, c'est traduire en clair en ne connaissant pas la clé. C'est donc l'espionne, ***Eve***, qui décrypte. Si elle y arrive, elle a brisé le secret d'Alice et Bob - elle aura réussi une ***cryptanalyse*** . L'opération ou son résultat s'appelle un **décryptement**.
Il importe évidemment de bien distinguer les deux. Tout l'objet de la cryptographie, c'est de rendre la première opération facile, et la deuxième impossible.

Déchiffrement

Action inverse du *chiffrement*, lorsque celui-ci est réversible : à l'aide d'un *algorithme cryptographique* et d'une *clé*, on reconstruit le *texte en clair* à partir du *texte chiffré*.

Décryptement, décryptage

Action qui consiste à *casser* le chiffrement d'un texte de façon à retrouver le *texte en clair* sans connaître la *clé* qui permet son *déchiffrement* normal.

Document primaire

Information originale, directe. Document de référence.

Encapsulage des clés

Technique par laquelle *une clé de session* est «enveloppée», c'est-à-dire chiffrée à l'aide d'une autre clé appartenant à un tiers (comme l'agent de récupération des clés). Dans les applications du courrier électronique, la clé enveloppée est généralement stockée dans l'entête du message. Dans les communications en temps réel, la clé enveloppée peut être transmise pendant le colloque de reconnaissance initiale qui établit une connexion confidentielle.

FAQ

Fichier questions-réponses. Acronyme anglais de Frequently Asked Questions désignant des fichiers de texte qui regroupent les questions les plus courantes sur un sujet donné.
En français, FAQ se traduit Foire Aux Questions.

Fonction de hachage

Aussi appelée **fonction de condensation**. Fonction qui convertit une chaîne de longueur quelconque en une chaîne de taille inférieure et généralement fixe ; cette chaîne est appelée empreinte (« digest » en anglais) ou condensé de la chaîne initiale.

Fonction de hachage à sens unique

Fonction de hachage qui est en plus une fonction à **sens unique** : il est aisé de calculer l'empreinte d'une chaîne donnée, mais il est difficile d'engendrer des chaînes qui ont une empreinte donnée. On demande généralement en plus à une telle fonction d'être sans collision, c'est-à-dire qu'il soit impossible de trouver deux messages ayant la même empreinte.

Fortran

FORmula TRANslator. Langage informatique. (1957)

Freeware

Logiciel gratuit, copiable à volonté mais dont l'auteur se réserve la propriété, le programme source n'étant pas modifiable.

FTP

(Protocole de transfert de fichiers). Protocole servant à déplacer ou transmettre des fichiers sur le réseau. Le protocole FTP permet d'établir une connexion à un autre site Internet et de télécharger ou d'envoyer des fichiers. Certains sites contiennent des fichiers du domaine public accessibles par FTP en entrant « anonymous » comme nom d'utilisateur et une adresse de courrier électronique comme mot de passe. Ce type d'accès est appelé FTP anonyme.

Hachage

Fonction mathématique qui permet de passer d'un grand (voire très grand) domaine à un domaine moindre. Elle peut être utilisée pour réduire un message qui serait trop long en une valeur de hachage ou une contraction du message qui est suffisamment compacte pour être utilisée comme donnée d'entrée dans un algorithme de signature numérique.

Intégrité

D'un point de vue cryptographique, assurer l'intégrité de données consiste à permettre la détection des modifications volontaires de ces données. L'intégrité n'est pas une signature. Voir *Signature.*

Langage C

Langage informatique. Conçu pour l'élaboration d'*Unix*, il tire son nom du langage B, utilisé pour créer la première version d'UNIX. Comme il est son descendant, il fut nommé C. (Dennis Ritchie - 1971)

Langage documentaire à structure combinatoire

Dans le langage documentaire à structure combinatoire, l'indexation s'effectue au niveau de chaque concept élémentaire où chacun de ces concepts et exprimé par un mot-clé. Pour la recherche, la combinaison des termes se fait pas les *opérateurs booléen.*

Langage Pascal

Langage informatique. Conçu par Nicklaus Wirth (1971) comme outil d'apprentissage de la programmation structurée.
(Le nom est un hommage à Blaise Pascal, et à sa machine à calculer).

Modèle OSI

Modèle de description des architectures réseaux en sept couches fonctionnelles. 1 - Physique, 2 - Liaison, 3 - - Réseau, 4 - Transport, 5 - Session, 6 - Présentation, 7 - Application.

Nombre premier

Un nombre premier est un nombre entier positif dont les seuls diviseurs sont 1 et lui-même. Les 26 nombres premiers inférieurs à 100 sont 1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Octet

Groupe de 8 *bits.*

Opérateur booléen

Georges Boole (1815-1864) a conçu une algèbre dite booléenne, très usitée en logique informatique. Les opérateurs booléen sont trois opérateurs binaires (et, ou, ou exclusif (*XOR*)) et un opérateur unaire (non).

OSI

Open Systems Interconnection. Voir aussi *Modèle OSI.*

Pertinence

Concerne le choix d'un mot-clé particulier par rapport au contenu du document du rôle assigné au mot clé en général.

PGP

PGP ("Pretty Good Privacy", soit "Plutôt bonne intimité"), élaboré par Phil Zimmermann, est sans doute le **logiciel de cryptographie le plus célèbre et le plus** controversé à l'heure actuelle.
Il est disponible par simple téléchargement à partir de dizaines de sites Internet à travers le monde, dans des versions Macintosh, MS-DOS, Windows, OS/2 et Unix. Il est gratuit pour l'usage non-commercial.

Son titre est une litote : utilisé correctement, PGP est **probablement indécryptable**, y compris par les services du Chiffre des grandes puissances. Autant dire qu'ils ne voient pas toujours d'un bon oeil sa prolifération.

Protocole

Ensemble de règles destinées à réaliser une communication.

SCSSI (Service Central de Sécurité des Systèmes d'Information)

SCSSI
18 rue du docteur Zamenhof
92131 ISSY LES MOULINEAUX CEDEX
Téléphone : 01.40 95 37 00 - Télécopie : 01 40 95 37 01
Le **SCSSI** est l'organisme chargé d'examiner les demandes d'autorisation des moyens et prestations cryptologiques en France. Il dépend directement du Premier Ministre. Installé au Fort d'Issy, son personnel est en grande partie militaire. Les critères selon lesquels il accorde ou refuse les autorisations sont secrets.

Shareware

Logiciel très bon marché, diffusé gratuitement pour essai et pour lequel l'auteur demande une rémunération symbolique ou l'envoi d'une carte postale.

Signature

C'est une donnée de taille faible qui, jointe à un message, prouve l'identité de l'émetteur du message. Si le message est modifié d'un seul bit, la signature change complètement. La signature est fonction du document signé (il ne faut pas que l'on puisse utiliser la même signature pour tous les documents) et fonction de votre clé publique. La signature assure en plus l'intégrité.

Silence

C'est le nombre de références pertinentes non décelées par le système documentaire.

TCP/IP

Architecture protocolaire fondée sur les protocoles TCP (Transport Control Protocol) et IP (InternetWork Protocol).

Texte chiffré

Aussi appelé *cryptogramme*. Données obtenues par application d'un *algorithme de chiffrement*. Le contenu sémantique de ces données n'est pas compréhensible.

Texte en clair

Données intelligibles, dont la sémantique est compréhensible.

Tiers de confiance

Responsable de la sécurité ou son agent à qui l'on fait confiance relativement à certaines activités liées à la sécurité. Souvent, l'expression est employée pour désigner une autorité de certification à laquelle quelqu'un d'autre que le propriétaire de données fait appel.

URL

Sigle de Uniform Resource Locator, méthode d'adressage indiquant le protocole des différents services disponibles dans le réseau Internet.

Unix

Système d'exploitation multi-processus, multi-utilisateurs dont les premières versions datent de 1969.

XOR

Ou exclusif : une chose ou l'autre, mais pas les deux.

5. Bibliographie

ALGORITHMIQUE GENERALE

[1] **BARBAROUX Paul**. *Principes d'une théorie générale de la sécurité algorithmique*. Thèse Doct. : Université d'Orsay. Paris, 1993. 138 p.

[2] **BECKETT Brian**. *Introduction aux méthodes de la cryptologie*. [1ère éd.]. Traduit de l'anglais par Philippe Béguin, Philippe Klein et Éric Henault. Paris ; Milan ; Barcelone : Masson, 1990. 332 p, 24 cm. ISBN 2-225-81941-6.

[3] **BECKETT Brian**. *Introduction to cryptolology and PC security*. [2ème éd. revue et augmentée]. New York : McGraw-Hill Pub., 1997. ISBN 0-077-09235-X.

[4] **BRASSARD Gilles**. *Cryptologie contemporaine*. Traduit de l'anglais par Claude Goutier ; rev. et actualisé par l'auteur. Paris ; Milan ; Barcelone : Masson, 1993. 124 p., 24 cm. ISBN 2-225-83970-0.

[5] **CHÉLY Pierre**. *Méthode originale d'écriture secrète : initiation à la cryptologie*. Paris, 1997. 235 p., 24 cm., 130 F. ISBN 2-85707-906-0.

[6] **DUBERTRET Gilles**. *Initiation à la cryptographie : manuel de cours, exemples et exercices résolus*. Vuibert. ISBN 2-7117-8632-3.

[7] **GIRAULT Marc**. *Analyse et conception d'algorithmes de cryptographie et de codage des données*. Thèse Doct. : Université de Caen. Caen, 1991. 318 p.

[8] **JOHNSON Bud**. *Break the code : cryptography for beginners*. Mineola, N.Y. : Dover Publications, 1997. 71 p., 28 cm. ISBN 0-486-29146-4.

[9] **MARSAULT Xavier**. *Compression et cryptage des données multimédias*. 2ème éd. revue et augmentée. Paris : Hermès, 1995. 243 p., 24 cm., 195 F. ISBN 2-86601-482-0.

[10] **PRENEEL Bart, RIJMEN Vincent**. *State of the art in applied cryptography : course on computer security and industrial cryptography*. Belgique : Leuven, 1997. ISBN 3-540-65474-7.

[11] **ROBIN Guy**. *Algorithmique et cryptographie*. Paris : Ellipses, 1992. 124 p., 24 cm., 150 F.

[12] **ROUBATY Romain**. *A.B.C. de cryptographie avec programme en Basic*. Paris : Masson, 1984. 207 p. ISBN 2-225-80443-5

[13] **SCHNEIER Bruce**. *Cryptographie appliquée : protocoles, algorithmes et codes source en C*. Trad. de Laurent Viennot. 2ème éd. Paris ; Albany [N.Y.] ; Bonn [etc.] : International Thomson publ. France ; New York : Wiley, 1996. 846 p., 24 cm. 340 F. ISBN 2-84180-036-9.

[14] **STINSON Douglas**. *Cryptographie : théorie et pratique*. Trad. de Serge Vaudenay. Paris ; Albany [N.Y.] ; Bonn [etc.] : International Thomson publ. France, 1996. 394 p., 24 cm., 260 F. ISBN 2-84180-013-X.

ALGORITHMIQUE SPECIFIQUE

♦ DATA ENCRYPTION STANDARD (DES)

[15] **BARKER Wayne G.** *Introduction to the analysis of the data encryption standard (DES)*. Laguna Hills, Californie : Aegean Park Press, 1991. 190 p., 28 cm. ISBN 0-894-12169-3.

[16] **BIHAM Eli**. *Differential cryptanalysis of the data encryption standard*. New York : Springer-Verlag, 1993. 188 p., 24 cm. ISBN 0-387-97930-1.

[17] **KATZAN Harry**. *The standard data encryption algorithm*. New York : PBI, 1977. 134 p., 24 cm. ISBN 0-894-33016-0.

[18] **SIMOVITS Mikael J.** *The DES, an extensive documentation and evaluation of the Data Encryption Standard*. Laguna Hills, Californie : Aegean Park Press, 1995. 116 p., 29 cm. ISBN 0-894-12248-7.

[19] **SMID Miles E., BRANSTAD Dennis**. The Data Encryption Standard : past and future. *Proceedings of the IEEE*, 1988, vol 76, n° 5, p. 550-560.

[20] **TAYLOR Jared**. The Data Encryption Standard. *PC Magazine*, 1977, vol 5, n°1, p. 180.

♦ RIVEST, SHAMIR, ADLEMAN (RSA)

[21] **BOYER R., MOORE J.S.** *Proof checking the RSA public key encryption algorithm*. Palo Alto, Californie : Morgan-Kaufmann, 1995. ISBN 0-934-61312-5.

[22] **COUTINHO S. C.** *The mathematics of ciphers : number theory and RSA cryptography*. Natick, Massachussets : A K Peters, 1998. ISBN 1-568-81082-2.

[23] **SEWELL, R.** Bulk encryption algorithm for use with RSA. *Electronics Letters*, 1993, vol 29, n° 25, p. 2183-2188.

[24] **SMITH Peter**. Cryptography without exponentiation; secure alternatives to RSA. (Encryption algorithms for data security). *Dr. Dobb's Journal*, vol 19, n° 4, p. 26-29.

[25] **WIRBEL Loring**. Public-key standard gets boost; National, others to support RSA cryptography algorithm. *Electronic Engineering Times*, 1994, n° 779, p. 4.

♦ BLOWFISH

[26] **SCHNEIER Bruce**. The blowfish encryption algorithm; a fast, new algorithm for 32-bit CPUs. *Dr. Dobb's Journal*, 1994, vol 19, n° 4, p. 38-42.

[27] **SCHNEIER Bruce**. The blowfish algorithm : one year later. (testing encryption algorithm for security). *Dr. Dobb's Journal*, 1995, vol 20, n° 9, p137-143.

♦ IDEA

[28] **SCHNEIER Bruce**. The IDEA encryption algorithm : an advanced block-cipher approach to encryption (the International Data Encryption Algorithm). *Dr. Dobb's Journal*, 1993, vol 18, n° 13, p. 50-57.

♦ RC5

[29] **RIVEST Ronald**. The RC5 encryption algorithm: a fast, symmetric block cipher that may replace DES. *Dr. Dobb's Journal*, 1995, vil 20, n° 1, p. 146-148.

PGP (PRETTY GOOD PRIVACY)

[30] **GARFINKEL Simson**. *PGP: pretty good privacy*. Sebastopol, Californie : O'Reilly & Associates, 1995. 393 p., 24 cm. ISBN 1-565-92098-8.

[31] **STALLINGS William**. *Protect your privacy : the PGP user's guide*. Englewood Cliffs, New Jersey : Prentice Hall PTR, 1995. 302 p., 21 cm. ISBN 0-131-85596-4.

[32] **ZIMMERMANN Philip**. *PGP source code and internals*. Cambridge, Massachussets : MIT Press, 1995. 907 p., 24 cm. ISBN 0-262-24039-4.

[33] **ZIMMERMANN Philip**. *The official PGP user's guide*. Cambridge, Massachussets : MIT Press, 1995. 216 p., 23 cm. ISBN 0-262-74017-6.

[34] **ZIMMERMANN Philip**. *Pretty good privacy 3.0 pre-alpha source code*. Palo Alto, Californie : Warthman Associates, 1996. 312 p., 28 cm. ISBN 0-964-96542-9.

DIVERS

[35] **GILBERT Henri**. *Cryptanalyse statistique des algorithmes de chiffrement et sécurité des schémas d'authentification*. Thèse Doct. : Université de Paris XI. Paris, 1997. 155 p.

[36] **LEVIEN Raph**. Protecting Internet E-mail from prying eyes. (includes related article on Internet E-mail encryption). *Data Communications*, 1996, vol 25, n° 6, p. 117-123.

[37] **NACCACHE David**. *Signatures numériques et preuves à divulgation nulle, cryptanalyse, défense et outils algorithmiques*. Thèse Doct. : Ecole Nationale Supérieure des Télécommunications. Paris, 1995. 146 p.

[38] **NEWTON David E.** *Encyclopedia of cryptology*. Santa Barbara, Californie : ABC-CLIO, 1997. ISBN 0-874-36772-7.

[39] **ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES (OCDE)**. *La politique de cryptographie*. OCDE, 1997. ISBN 92-64-26023-4.

[40] **RADOSEVICH Lynda**. E-mail security choices to expand. (vendors support multiple encryption algorithms). *InfoWorld*, 1997, vol 19, n° 36, p. 10-11.

[41] **SCHNEIER Bruce**. A taxonomy of encryption algorithms. *Computer Security Journal*, 1993, vol 9, n° 1, p. 39-60.

[42] **SCHNEIER Bruce**. Clipper gives Big Brother far too much power. (National Security Agency encryption chip). *Computerworld*, 1993, vol 27, n° 22, p. 33.

[43] **SMITH Richard E.**. *Internet cryptography*. Massachussetts : Reading, 1997. ISBN 0-201-92480-3.

[44] **STERN Jacques**. *La science du secret* - Paris : O. Jacob, 1998. 203 p., 22 cm. ISBN 2-738-10533-5.

[45] **TARMAN T., HUTCHINSON R., PIERSON L., SHOLANDER P., WIRZKE E.** Algorithm-agile encryption in ATM networks. *Computer*, 1998, vol 31, n°.9, p.57-64.

[46] **TRUE James**. Evaluating frame-relay encryption systems. (includes related article on available encryption algorithms). *M. Telecommunications*, 1996, vol 30, n° 12, p. 62-64.

INTERNET

GENERALITES SUR LA CRYPTOGRAPHIE - ALGORITHMES CONFONDUS

[47] http://www.counterpane.com/
Site de Bruce Schneier. Etat de l'art de la cryptologie, liens, FAQ, environ 950 articles de journaux et de conférences depuis 1978 téléchargeables au format PDF, Postscript ou Word 97 , FTP, algorithmes, informations diverses. Excellent site.

[48] http://www.rsa.com/
Site américain des laboratoire RSA (RIVEST, SHAMIR et ADLEMAN).

[49] http://web.mit.edu/
Site du Massachussetts Institute Technology (MIT), université américaine. On y trouve énormément d'informations dans le domaine.

[50] http://mitpress.mit.edu/
Centre de presse du Massachussetts Technology Institute (MIT) : recherche d'articles de journaux et de monographies. Excellent site.

[51] http://www.cryptography.com/
Site américain de recherche sur la cryptographie. Présentations de différentes recherches et informations, notamment sur le DES, RSA et le protocole SSL.

[52] http://www.cis.ohio-state.edu/
Site de l'université d'Ohio.

[53] http://web.cnam.fr/www2/cours/crypto/cryptographie.html

[54] http://www.cnam.fr/reseau/Crypto/
Site du Conservatoire Nationale des Arts de Métiers (C.N.A.M.). Cours sur les algorithmes et l'utilisation du chiffrement en France. Nombreux liens. Très bon site.

[55] http://world.std.com/~franl/crypto/
Site américain : FAQ, liens sur des articles de presse et livres, informations générales sur la cryptographie. Site très complet.

[56] http://www.eff.org
Electronic Frontier Fondation est le laboratoire américain qui a construit Deep Crac pour le Challenge DES III.

[57] http://www.iacr.org/
Site de l'International Association for Cryptologic Research (I.A.C.R.). Organisation scientifique qui propose des travaux de recherche en matière de cryptologie. On y trouve le détails de conférences, le calendrier des événements, des publications et diverses informations. Son journal officiel est The *Journal of Cryptology*. Excellent site.

[58] http://www.adminet.com/min/pm/crypto.html
Site français d'informations générales.

[59] http://www.ssh.fi/tech/crypto/
Site de la société américaine de sécurité sur internet, créatrice du protocole SSH. Site très complet sur les algorithmes, les protocoles, les bibliographies avec des liens sur des FAQ, des listes de discussions, des FTP et d'autres sites.

[60] http://csrc.nist.gov/encryption/
Site du National Institute of Standards and Technology (N.I.S.T.). Description des algorithmes AES, Skipjack et KEA, DES, Triple DES, RSA. Possibilité de téléchargement au format PDF.

[61] http://www.crypto.com/
Site américain d'informations générales sur la cryptologie.

[62] http://www.crypto.org/
Site américain d'informations générales sur la cryptologie.

[63] http://www.distributed.net/
Dite de la société qui a cassé DES 56 bits - FAQ.

[64] http://www.dice.ucl.ac.be/crypto/
Site général sur la cryptologie. Cours sous forme de transparents (protocoles et algorithmes) de l'Université Catholique de Louvain. Site en français et en anglais.

[65] http://urec.fr/
Le moteur de recherche de l'UREC (unité de réseau du CNRS) est consacré à l'Enseignement et à la Recherche en France. Il indexe les sites des écoles, universités, instituts de formation et de recherche, laboratoires de recherche etc.

[66] http://www-ensimag.imag.fr/eleves/Remi.Zara/tipe/crypto/somm.html
Page de cours sur la cryptographie de l'Ecole Nationale Supérieure d'Informatique et de Mathématiques Appliquées de Grenoble (E.N.S.I.M.A.G.). Concerne surtout l'algorithme R.S.A.

[67] http://www-telesun.imag.fr/cours/securite/introduction/crypto.htm
Cours sur le DES et RSA du laboratoire de l'IMAG, fédération d'Unités de Recherche du CNRS, de l'INPG et de l'Université Joseph Fourier de Grenoble.

[68] http://messel.emse.fr/~gsoler/cryptog.html
Page sur les algorithmes de cryptage des étudiants de l'Ecole des Mines de Saint-Etienne.

[69] http://www.droit.umontreal.ca/faculte/fr/informations/infoetud/cours/drt3307/cours3.html
Site francophone sur les algorithmes de cryptologie de la faculté de droit de l'université de Montréal.

[70] http://www.dmi.ens.fr/equipes/grecc/
Site du Groupe de Recherche En Complexité et Cryptographie (G.R.E.C.C.) du Département de Mathématiques de l'Informatique (D.M.I.) de l'Ecole Nationale Supérieure (E.N.S.).

[71] http://wwwusers.imaginet.fr/~dohm/crypto_fr.html
Site non référencé sur les algorithmes de cryptage et la législation française. Bibliographie, liens et possibilité de téléchargement.

[72] http://www.geocities.com/Paris/Palais/6219/index.html
Site non référencé, d'informations générales.

PAGES SPECIFIQUES SUR LES ALGORITHMES

♦ IDEA

[73] http://www.ascom.ch/Web/systec/security/idea.htm
La société américaine Ascom Systec détient les propriétés intellectuelles sur IDEA. Téléchargement des diverses versions du logiciels IDEA.EXE (avec source C) utilisant l'algorithme.

[74] ftp://idea.sec.dsi.unimi.it/pub/security
FTP IDEA

♦ MD5

[75] http://theory.lcs.mit.edu/~rivest/rfc1321.txt
L'algorithme MD5, par le site Massachussetts Technology Institute (MIT).

♦ Blowfish

[76] http://www.counterpane.com/blowfish.html
L'algorithme Blowfish de Bruce Schneier sur le site de sa société.

SITES SPECIFIQUES AUX LOGICIELS DE CHIFFREMENT

♦ P.G.P. (Pretty Good Privacy)

[77] http://www.pgp.com/
Site de la société Pretty Good Privacy, Inc. de Philip ZIMMERMANN. Site de commercialisation des versions et d'informations sur la cryptologie.

[78] http://www.pgpi.com/
Site international de PGP.

[79] http://web.mit.edu/network/pgp.html
Sites du Massachusetts Institute Technology (MIT). Page de référence du M.I.T. concernant PGP.

[80] http://www.mit.edu:8001/people/warlord/pgp-faq.html
[81] http://web.mit.edu/afs/net/mit/jis/www/pgpfaq.html
FAQ du Massachussetts Institute Technology (MIT) sur PGP.

[82] http://www.pgp.net/
Informations PGP et FAQ.

[83] http://world.std.com/~franl/pgp/
Site américain sur PGP.

[84] http://www.in4mation.de/pgp/epgp.index.html
Site en anglais de la société Allemand Online In4mation Ist.

[85] http://www.geocities.com/SiliconValley/Bay/9648/intimite.htm
Site non référencé sur PGP.

[86] http://www.info.fundp.ac.be/~telecom/telecom/pgp/pgp.htm
Site des Facultés Universitaires Notre Dame de la Paix de NAMUR - Cours sur PGP.

[87] http://www.fortunecity.com/skyscraper/oracle/598/
Télécharger PGP version FRANCAISE (clé de 40 bits).

[88] http://www.geocities.com/SiliconValley/Bay/9648/intimite.htm
Informations sous forme de FAQ et télécharger PGP version FRANCAISE (clé de 40 bits).

[89] http://www.cis.ohio-state.edu/hypertext/faq/usenet/pgp-faq/where-is-PGP/faq.html
FAQ du site de l'université d'Ohio concernant PGP.

SERVEURS FTP

[90] ftp://ftp.pgpi.com/pub/pgp/6.0/6.0.2i/
Téléchargement du code source de PGP 6.02 en version Windows et Mac
[91] ftp://ftp.csua.berkeley.edu/pub/cypherpunks/pgp
[92] ftp://ftp.funet.fi/pub/crypt/cryptography/pgp
[93] ftp://ftp.dsi.unimi.it/pub/security/crypt/PGP

La loi interdit formellement d'importer un logiciel de cryptographie à partir d'un pays extérieur à la CE, sans une autorisation du Premier Ministre. Mais l'importation à partir des pays suivants est libre : Allemagne, Italie, Suède, Pays-Bas (2), Suède, Royaume-Uni.

[94] ftp://ftp.cert.dfn.de/pub/pgp/
[95] ftp://idea.sec.dsi.unimi.it/pub/security/crypt/PGP
[96] ftp://ftp.funet.fi/pub/crypt/pgp/
[97] ftp://ftp.nl.net/pub/crypto/pgp

[98] ftp://ftp.nic.surfnet.nl/surfnet/net-security/encryption/pgp
[99] ftp://leif.thep.lu.se
[100] ftp://sable.ox.ac.uk/pub/crypto/pgp

[101] news:alt.security.pgp
Forum anglais sur PGP.

TELECHARGEMENT DE LOGICIELS DE CRYPTAGE (sauf PGP) ET PROTOCOLES

[102] http://www.msi-sa.fr/
Site de la société française MSI (Méthode et Solution Informatique). Possibilité de télécharger gratuitement une version d'évaluation de 30 jours du logiciel Security Box.

[103] http://32bit.bhs.com/
Beverly Hills Software. Site américain spécialisé dans le téléchargement de toute sortes de logiciels gratuits : moteur de recherche, index des logiciels par ordre alphabétique du nom. Téléchargement de Blowfish, PGP, etc.

[104] http://www.fortunecity.com/skyscraper/oracle/598/crypto.htm
Télécharger des logiciels de sécurité freeware. Plusieurs liens sur des sites non référencés.

[105] http://home.netscape.com/newsref/std/sslref.html
Netscape Communications rend gratuite la distribution du code source de SSL à son site.

[106] ftp://ftp.funet.fi/pub/unix/security/login/SSL
Ftp pour télécharger SSL pour UNIX.

LES PROTOCOLES

- **SSL**

[107] http://help.netscape.com/products/server/enterprise/3x/manual/encrypt.htm
Site Netscape (en Anglais).

[108] http://www.epfl.ch/SIC/SA/publications/FI95/fi-7-95/7-95-page3.html
Site en francophone de l'Ecole Polytechnique Fédérale de Lausanne.

[109] http://home.netscape.com/products/security/ssl/index.html
FAQ, explications sur le protocole SSL, autres.

[110] ftp://ftp.psy.uq.oz.au/pub/Crypto/SSL/
ftp SSL.

- **SSH**

[111] http://www.ssh.fi/
Site officiel SSH en anglais.

LEGISLATION FRANÇAISE EN MATIERE DE CRYPTOLOGIE

[112] http://www.internet.gouv.fr/francais/textesref/guidepratique.htm
Site du programme d'action gouvernemental pour la société de l'information. Guide pratique de la réglementation française.

[113] http://www.journal-officiel.gouv.fr/
[114] http://www.telecom.gouv.fr/francais.htm
Site officiel du Gouvernement.

[115] http://www.telecom.gouv.fr/francais/activ/telecom/nloi1a5.htm
Loi de réglementation des télécommunications (n° 96-659 du 26 juillet 1996 - Journal Officiel du 27 juillet 1996).

[116] http://www.telecom.gouv.fr/francais/activ/telecom/deccrypto1.htm
Décret no 98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie.

[117] http://www.telecom.gouv.fr/francais/activ/telecom/deccrypto2.htm
Décret no 98-102 du 24 février 1998 définissant les conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui des conventions secrètes de cryptologie en application de l'article 28 de la loi no 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications.

[118] http://www.telecom.gouv.fr/francais/activ/techno/crypto0698_1.htm
La réglementation française en matière de cryptologie. Document téléchargeable aux formats Word et RTF.

[119] http://www.internet.gouv.fr/francais/textesref/cisi190199/decis1.htm
Décision gouvernementale en matière de cryptologie du 19/01/1999.

[120] http://www.premier-ministre.gouv.fr/PM/D190199.HTM
Discours et interventions - Conférence de presse de Monsieur Lionel JOSPIN, Premier Ministre, à l'issue du Comité interministériel pour la société de l'information Hôtel de Matignon Mardi 19 janvier 1999.

[121] http://www.iris.sgdg.org/axes/crypto/
Association IRIS pour le droit au chiffrement (association française loi 1901).

[122] http://www.argia.fr/lij
L'Internet Juridique. Site dédié aux aspects juridiques de l'Internet. Il est destiné aussi bien aux professionnels du droit qu'aux entreprises. Créé février 1996, il est l'un des plus anciens sites web français à thème juridique. On y trouve des articles de fond, des informations sur la cryptographie, un panorama de la jurisprudence française en matière d'Internet. Son catalogue de ressources recense les sites web juridiques français classés par thème et comporte des liens vers des sites étrangers, notamment francophones, les plus intéressants.

[123] http://www.planete.net/~jbaagoe/loi_crypto.html
La réglementation de la cryptologie (la page de Johannes Baågøe). Beaucoup de sites référencent cette page.

[124] http://www.scssi.gouv.fr/present/si/ccsti/ccsti5.html
Site du SCSSI (Service Central de la Sécurité des Systèmes d'Information).

FORUMS DE DISCUSSIONS (NON-SPECIFIQUES)

- Forum en français.

[125] news:fr.misc.cryptologie
[126] news:fr.comp.securite
[127] news:sci.crypt

- Forum en anglais.

[128] news:sci.crypt
[129] news:sci.crypt.research
[130] news:talk.politics.crypto
[131] news:sci.answers
[132] news:news.answer
[133] news:alt.security
[134] news:alt.security.index

F.A.Q. (Frequently Asked Questions) généralistes

[135] http://www.pgpi.com/faq/
FAQ du site de pgpi.com.

[136] http://www.rsa.com/rsalabs/faq/index.html
FAQ du site rsa.com. Moteur de recherche et possibilité de téléchargement au format PDF.

[137] http://www.jurisva.com/ialta/Faqcrypt.htm
FAQ française du site de services extranet à valeur ajoutée dédié au monde du droit, professionnels et utilisateurs, national et international.

[138] http://www.aui.fr/aui/Projets/Crypto/
Site française de l'AUI : ASSOCIATION DES UTILISATEURS D'INTERNET.
Association à but non lucratif créée le 12/02/1996 publiée au JO N° 1416 (13/03/1996).
FAQ française sur la cryptographie. Possibilité de télécharger la FAQ sous différents formats.

[139] http://www.cis.ohio-state.edu/hypertext/faq/usenet/FAQ-List.html
Ohio State University : ce site permet la recherche par mot-clé ou un balayage des noms de FAQ classées alphabétiquement.

[140] http://www.cis.ohio-state.edu/hypertext/faq/usenet/cryptography-faq/top.html
FAQ de l'université d'ohio (Ohio State University) sur la cryptographie.

[141] http://www.sri.ucl.ac.be/SRI/F50i.html
La FAQ officielle de PGPi (traduite en français par Jean-Pierre Kuypers).

FTP - FAQ

[142] ftp://rtfm.mit.edu/pub/usenet/news.answers/cryptography-faq/
FAQ du Massachussetts Institute Technology (MIT) sur la cryptographie.

[143] ftp://rtfm.mit.edu/pub/usenet/sci.crypt/
[144] ftp://rtfm.mit.edu/pub/usenet/sci.crypt.research/
FAQ du Massachussetts Institute Technology (MIT) : Cryptographie générale - RSA - SSL.

FTP

[145] ftp://ftp.funet.fi/pub/crypt
[146] ftp://ftp.kfki.hu/pub/packages/security
[147] ftp://ftp.kiae.su/pub/unix/crypto
[148] ftp://ftp.ox.ac.uk/pub/crypto
[149] ftp://ftp.psy.uq.oz.au/pub/Crypto (DES et SSL)
[150] ftp://ftp.sunet.se/pub/security/tools/crypt
[151] ftp://ftp.uni-mainz.de/pub/internet/security/SSL/ (site SSL)
[152] ftp://ftp.unit.no/pub/unix/security
[153] ftp://garbo.uwasa.fi/pc/crypt
[154] ftp://gwynne.cs.ualberta.ca/pub/Crypto/ (DES et SSL)
[155] ftp://pgp.rasip.fer.hr/pub/crypt
[156] ftp://utopia.hacktic.nl/pub/replay/pub/disk
[157] ftp://ftp.replay.com/replay/mirror/
[158] ftp://ftp.darmstadt.gmd.de

6. Index

7. Annexes

ANNEXE 1 : ARITHMETIQUE MODULO

ANNEXE 2 : LES ETAPES DU DES (DATA ENCRYPTION STANDART)

ANNEXE 3 : EXEMPLE DE CHIFFREMENT RSA

ANNEXE 4 : LES SEQUENCES D'EVENEMENTS DE L'ALGORITHME IDEA

ANNEXE 5 : DESCRIPTION DE L'ALGORITHME MD5

ANNEXE 6 : LES ETAPES DE L'ALGORITHME BLOWFISH

ANNEXE 7 : PHOTO DE DEEP CRACK

ANNEXE 1 : ARITHMETIQUE MODULO

On a tous appris l'arithmétique modulo n[9] à l'école. ; cela s'appelait l'arithmétique de l'horloge :

« Si « A » dit qu'il sera à la maison pour 10 heures et qu'il rentre 13 heures plus tard, à quelle heure rentre-t-il à la maison et quel est l'âge du capitaine ? ».

C'est la l'arithmétique modulo 12. La réponse se calcule de la manière suivante :

$$(10 + 13) \bmod 12 = 11$$

Ce qui s 'écrit aussi comme la **congruence** :

$$(10 + 13) \equiv 11 \pmod{12}.$$

La notation **a ≡ b (mod n)** indique **a = b + kn** pour un certain entier **k**. Si **a** et **b** sont positifs et si **b** est plus petit que **n**, on peut considérer que :

b est le **reste de la division** de **a** par **n**.

On a aussi la propriété que **a** et **b** donnent le même reste quand ils sont divisés par **n**. Parfois **b** est appelé le **résidu** de **a modulo n**. On dit aussi que a est **congru** à **b modulo n** (le symbole ≡ dénote une congruence). Ce ne sont que des différentes manières de dire la même chose.
L'ensemble des **entiers** de **0** à **n - 1** forme ce que l'on appelle **l'ensemble de tous les résidus modulo n**. Ce qui signifie que, pour tout entier quelconque **a**, son résidu modulo n est un nombre compris entre **0** et **n - 1** bornes comprises.
L'opération **a mod n** dénote le résidu **a**. Ce résidu est un **nombre entier** compris entre **0** et **n - 1**. Cette opération est parfois appelée la **réduction modulo n**. Par exemple, **5 mod 3 = 2**.

Attention, cette définition de « mod » peut être différente de celle qui est utilisée dans certains langages de programmation. Par exemple, l'opérateur modulo du langage *Pascal* fournit parfois un résultat négatif. Dans ce cas, le résultat est compris entre -n - 1 et n - 1. Il en va aussi différemment dans le *langage C*.

Tout comme l'arithmétique classique, l'arithmétique modulo n jouit des propriétés de commutativité, d'associativité et de distributivité :

```
(a + b) mod n = ((a mod n) + (b mod n)) mod n
(a - b) mod n = ((a mod n) - (b mod n)) mod n
(a x b) mod n = ((a mod n) x (b mod n)) mod n
(a x b (b +c)) mod n = (((a x b) mod n) + ((a x c) mod n)) mod n
```

ANNEXE 2 : LES ETAPES DU DES (DATA ENCRYPTION STANDART)

Les étapes du DES sont les suivantes [2][13][53][67] :

Etape 1 - Permutation initiale : Le bloc de 64 bits est divisé en 2 blocs (G et D : Gauche et Droite) de 32 bits qui sont permutés d'après la table de permutation suivante :

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Le bit 58 est remplacé par le bit 1, le bit 50 par le bit 2, le bit 42 par le bit 3, ... le bit 64 par le bit 7.

Etape 2 - Génération des clés : Initialement, la clé de 64 bits est réduite à 56 en ignorant un bit sur huit. Cela se fait par la table de permutation de clé suivant :

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Une fois la clé de 56 bits extraite, on effectue 16 rondes (une ronde est une substitution suivie d'une permutation basée sur la clé) d'opérations identiques dans lesquelles les données sont combinées avec la clé.

A chaque ronde, les bits de la clé Ki sont décalés, puis 48 bits sont sélectionnés parmi les 56 bits de la clé. Cette opération se fait de la façon suivante : les 56 bits sont divisés par 2 moitiés de 28 bits. Les moitiés sont décalées vers la gauche d'une ou de deux positions selon la table de décalage de clé suivante :

Ronde	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Nb décalage	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	2

Après avoir été décalés, 48 bits sont sélectionnés parmi les 56 selon une permutation compressive. Le tableau ci-dessous définit la permutation compressive. Par exemple, le bit en position 33 de la clé décalée va en position 35 de la sortie, et le bit en position 18 de la clé décalée est ignoré.

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Etape 3 - Permutation expansive : Les bloc D (bloc de droite de données) de 32 bits est alors étendu à 48 bits par une permutation expansive. Pour chaque bloc d'entrée de 4 bits, le 1er et le 4ème constituent deux bits de sortie, le 2ème et le 3ème un bit de sortie. Ce cette manière, les bits 32 bits sont rangés de la façon suivante :

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Les bits 1,4,5,8,9,12,13,16,17,10,21,24,25,28,29,32 ont été doublés, soit 16 bits de plus que les 32 bits initiaux, soit 48 bits.

Etape 4 : On réalise alors un **OU EXCLUSIF** (***XOR***) entre les 48 bits de la clé Ki (i de 1 à 16) (étape 2) et les 48 bits du bloc Di que l'on vient de générer (étape3).

Etape 5 - Substitution par table-S : Les 48 bits de l'étape 4 sont remplacés par 32 bits après passage dans l'une des 8 tables de substitution appelées tables-S.
Les 48 bits sont découpés en 8 blocs de 6 bits. Chaque bloc est manipulé séparément par une table-S différente : le bloc 1 par la table-S 1, le bloc 2 par la table-S 2, etc.

Tables-S

S1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2

15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3

10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6

12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7

4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8

13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Etape 6 - Permutation-P : Les 32 bits de sortie des substitutions par tables-S sont permutés à l'aide de la table-P. ci-dessous :

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	21	14	32	27	3	9	19	13	30	6	22	11	4	25

Cette table met en correspondance chaque bit de l'entrée avec un bit de sortie. Par exemple, le bit 16 va en position 1, le bit 21 va en position 4, le bit 6 en position 28 et le bit 25 va en position 32.

Le résultat de la permutation-P des 32 bits est combiné avec un OU EXCLUSIF avec les 32 bits du bloc de gauche (dont on ne s'était pour l'instant jamais occupé). On obtient un nouveau bloc de 32 bits

Etape 7 : Les blocs G (resté identique à celui de l'étape 1) et le bloc D (après étape 6) sont inversés et une nouvelle ronde commence.

N.B. : la deuxième ronde transformera ce coût-ci le bloc G passé à droite et maintiendra le nouveau bloc modifié après les 7 étapes. De ce fait, à chaque ronde, le bloc G n'est jamais modifié.

Etape 8 - Permutation finale : Après les 16 rondes, on observe une permutation finale sur les 64 bits obtenus par concaténation des 32 bits G et D. C'est 64 bits sont permutés selon la table ci-dessous :

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Cette table est la matrice inverse de la table de permutation initiale présentée dans l'étape 1.

Déchiffrement du DES

L'algorithme de déchiffrement est exactement le même que celui du chiffrement. La seule différence est que les clés doivent être utilisées dans l'ordre inverse. Si les clés de chiffrement de chaque ronde sont K1, K2, ..., K16, alors les clés de déchiffrement sont K16, K15, ..., K1.

ANNEXE 3 : EXEMPLE DE CHIFFREMENT RSA

Exemple de chiffrement RSA : [13]

Si **p = 47** et **q = 71** alors : **n = p x q = 3337**

La clé de chiffrement **e** ne doit pas avoir de facteur commun avec : **(p - 1) x (q - 1) = 46 x 70 = 3220**

Choisir **e** (aléatoirement) égal = **79**. Dans ce cas : $d = 79^{-1} \bmod 3220 = 1019$

Pour chiffrer le message **m = 688232687966683**, divisons le d'abord en petit bloc de trois chiffres. Le message est divisé en 6 blocs m_i tels que : $m_1 = 668$, $m_2 = 232$, $m_3 = 687$, $m_4 = 796$, $m_5 = 668$, $m_6 = 3$

Le premier bloc est chiffré $688^{79} \bmod 3337 = 1570 = c_1$

En effectuant la même opération pour les autres blocs, on obtient le message chiffré :

C = 1570 2756 2091 2276 2423 158

Pour déchiffrer le message, il faut effectuer les mêmes exponentiations mais en utilisant la clé de déchiffrement $1570^{1019} \bmod 3337 = 688 = m_1$

N.B. :

- le calcul de **d** qui est l'**inverse** de **a modulo n** est un problème difficile à résoudre. Il est résolu à l'aide de **l'algorithme d'Euclide étendu**.
- $1570^{1019} \bmod 3337$ tel que, est incalculable puisque 1570^{1019} est trop grand. On décomposera la puissance en puissances de 2.
  Par exemple, $a^{16} \bmod n = (((a^2 \bmod n)^2 \bmod n)^2 \bmod n)^2 \bmod n$

ANNEXE 4 : LES SEQUENCES D'EVENEMENTS DE L'ALGORITHME IDEA

A chaque ronde, la séquence d'événements est la suivante :

1. On multiplie X*1* avec le premier bloc de clé *Z1 (X1 * Z1)*
2. On additionne X*2 avec* Z*2 (X2 + Z2)*
3. X*3* + Z*3*
4. X*4* * Z*4*
5. (Etape 1) XOR (Etape 3)
6. (Etape 2) XOR (Etape 4)
7. (Etape 2) * Z*5*
8. (Etape 6) + (Etape 7)
9. (Etape 8) * Z*6*
10. (Etape 7) + (Etape 9)
11. (Etape 1) XOR (Etape 9) => X*1* de la ronde suivante
12. (Etape 3) XOR (Etape 9) => X*3* de la ronde suivante
13. (Etape 2) XOR (Etape 10) => X*2* de la ronde suivante
14. (Etape 4) XOR (Etape 10) => X*4* de la ronde suivante

Il y aura de plus 4 étapes supplémentaires après la huitième ronde :

1. X*1* * Z*1* (X1 est le résultat de l'étape 11 de la première ronde)
2. X*2* + Z*2* (X2 est le résultat de l'étape 12 de la première ronde)
3. X*3* + Z*3* (X3 est le résultat de l'étape 13 de la première ronde)
4. X*4* * Z*4* (X4 est le résultat de l'étape 14 de la première ronde)

Ces 4 blocs sont rassemblés pour former le texte chiffré.

Création de clés dérivées :
Par ailleurs il n'y aura pas 6 clés uniques mais 52 clés dérivées (6 pour chacune des 8 rondes + 4 pour la transformation finale). La clé de 128 bits sera divisée en 8 blocs de 16 bits, constituant les 8 premières clé dérivées parmi les 52. La clé de 128 bits sera alors ensuite décalée circulairement vers la gauche de 25 bits et donnera 8 nouveaux blocs de 16 bits. Et ainsi de suite jusqu'à la fin de l'algorithme.

ANNEXE 5 : DESCRIPTION DE L'ALGORITHME MD5

En premier lieu, le message en clair est complété de manière à ce que 64 bits de plus amèneraient sa longueur à un multiple de 512. Ce remplissage se fait avec un seul 1 rajouté à la fin du message suivi d'autant de 0 que nécessaire.
Ensuite, une représentation de 64 bits de la longueur totale du message (avant que le remplissage ne soit effectué) est jointe au résultat.

Ces deux étapes servent à rendre la longueur du message multiple de 512 bits (ce qui est nécessaire pour la suite de l'algorithme), tout en s'assurant que des messages différents n'auront pas l'air similaires après le remplissage.

Quatre variables de 32 bits sont initialisées :
A = 0x01234567
B = 0x89ABCDEF
C = 0xFEDCBA98
D = 0x76543210
On les appelle "variables de chaînage".

Maintenant, la boucle principale de l'algorithme commence. Cette boucle est effectuée autant de fois qu'il y a de blocs de 512 bits dans le message à traiter.
Les quatre variables sont copiées dans d'autre variables A dans AA, B dans BB, C dans CC et D dans DD.
La boucle principale a 4 rondes (MD4 n'avait que 3 rondes), toutes très similaires.
Chaque ronde consiste en 16 exécutions d'une opération. Chaque opération calcule une fonction non linéaire de trois des variables A, B, C et D. Ensuite, elle ajoute au résultat la quatrième, un sous-bloc et une constante. Ce nouveau résultat est ensuite décalé circulairement vers la gauche d'un nombre variable de bits et ensuite ajouté à l'une des A, B, C, D. Finalement ce dernier résultat remplace l'une des A, B, C, D.

Il y a 4 fonctions non linéaires, une différente pour chaque ronde :
F(X,Y,Z) = X.Y + (Not X).Z
G(X,Y,Z) = X.Z + (Not Z).Y
H(X,Y,Z) = X Xor Y Xor Z
I(X,Y,Z) = Y Xor ((Not Z) + X)
Not, ., +, Xor étant les opération habituelles sur les booléens.
Ces fonctions sont conçues de telle manière que si les bits correspondants de X, Y et Z sont indépendants et non biaisé, alors les bits du résultat sont aussi indépendants et non biaisés. La fonction F est la conditionnelle bit à bit : si X, alors Y, sinon Z. La fonction H est l'opérateur de parité bit à bit.

Si Mj représente le j° sous-bloc du message (j allant de 0 à 15), et si << S représente un décalage circulaire à gauche de S bits, les quatre opérations de base sont :
FF(a,b,c,d,Mj,s,Ti) dénote a = b + ((a + F(b,c,d) + Mj + Ti) << S);
GG(a,b,c,d,Mj,s,Ti) dénote a = b + ((a + G(b,c,d) + Mj + Ti) << S);
HH(a,b,c,d,Mj,s,Ti) dénote a = b + ((a + H(b,c,d) + Mj + Ti) << S);
II(a,b,c,d,Mj,s,Ti) dénote a = b + ((a + I(b,c,d) + Mj + Ti) << S);
Les Ti peuvent être choisies de la manière suivante :
A l'étape i, Ti est la partie entière de 2^32 * abs (sin (i)), où i est exprimé en radian.

Après tout cela, A, B, C et D sont ajoutées à AA, BB, CC, DD respectivement et l'algorithme continue avec le bloc suivant de données. Le résultat final est la jointure de AA, BB, CC, DD.

ANNEXE 6 : LES ETAPES DE L'ALGORITHME BLOWFISH

1. P-array = 18 sous-clés de 32-bits. P1, P2,..., P18
2. Il y a 4 S-boxes de 32 bits avec 256 entrées chacune :
   S1,0, S1,1,..., S1,255;
   S2,0, S2,1,..., S2,255;
   S3,0, S3,1,..., S3,255;
   S4,0, S4,1,..., S4,255.

La méthode pour calculer ces sous-clés est décrite après.

Chiffrage :

16 tours. L'entrée x est un élément de 64 bits. On divise x en 2 parties de 32 bits : xL et xR
Pour i = 1 à 16
xL = xL XOR Pi
xR = F(xL) XOR xR
Inverser xL et xR
Inverser xL et xR (Annuler la dernière inversion)
xR = xR XOR P17
xL = xL XOR P18
Recombiner xL et xR

Fonction F :
Diviser xL en 4 quart de 8 bits : a, b, c, et d
$F(xL) = ((S1,a + S2,b \bmod 2^{32}) \text{ XOR } S3,c) + S4,d \bmod 2^{32}$

Le déchiffrement est exactement la même chose, à l'exception que P1, P2, ..., P18 sont utilisés dans l'ordre inverse.

Génération des sous-clés :

Les sous-clés sont calculées en utilisant l'algorithme Blowfish. La méthode exacte suit :

1. On initialise en premier le P-array et ensuite les 4 S-boxes, dans l'ordre, avec une chaîne fixe. Cette chaîne est constituée de chiffre hexadécimaux de Pi (moins le 3 initial). Par exemple :
   P1 = 0x243f6a88
   P2 = 0x85a308d3
   P3 = 0x13198a2e
   P4 = 0x03707344
2. On exécute un XOR entre P1 et les 32 premiers bits de la clé, un XOR P2 avec les 32 bits suivants de la clé, ainsi de suite pour tous les bits de la clé.
   On répète le cycle jusqu'à que tous le P-array soit « XORé » avec les bits de la clé.
   Pour toutes les petites clés, il y a au moins une clé de longueur équivalente. Par exemple, si A est une clé de 64 bits, alors AA, AAA, etc., sont également des clés.
3. Chiffrer toutes les chaînes vides avec l'algorithme Blowfish, en utilisant les sous-clés est décrit dans les étapes (1) et (2).
4. Remplacer P1 et P2 avec la sortie de l'étape (3).
5. Chiffrer la sortie de l'étape (3) en utilisant l'algorithme Blowfish avec les sous-clés modifiées.
6. Remplacer P3 et P4 avec la sortie de l'étape (5).
7. Continuer les processus en remplaçant toutes les entrées du P-array, et après les 4 S-boxes dans l'ordre, avec la sortie de l'algorithme Blowfish.

Au total, 521 itérations sont nécessaires pour générer toutes les sous-clés.

ANNEXE 7 : PHOTO DE DEEP CRACK

Deep Crack de l'EFF (Electronic Frontier Fondation) [56] a cassé la clé de 56 bits de l'algorithme DES en 22 heures 15 minutes