COLLOQUE NATIONAL SUR LE TRAITEMENT DU SIGNAL
ET SES APPLICATIONS

NICE du 26 au 30 AVRIL 1977

PROTECTION DU SECRET PAR CHIFFREMENT DANS UN RESEAU PUBLIC A COMMUTATION DE DONNEES PAR PAQUETS.

Louis GUILLOU - Sami HARARI - Bernard LORIG

C.C.E.T.T. , Département RSI, 2, rue de la Mabilais - B.P. 1266 35013 RENNES CEDEX

RESUME

L'extension de la téléinformatique pose le problème de la protection des données contre d'éventuelles malveillances lors de leur transmission ou de leur stockage.

Comme corollaire se pose aussi le problème de l'identification du terminal ou de la personne désirant accéder à ces données. La solution à ces problèmes se trouve dans l'utilisation des codes protégeant le secret des données et des identités respectives. C'est ainsi un problème de cryptage.

Dans la première partie nous recensons les menaces sur un système téléinformatique , ainsi que les 2 classes de codes cryptographiques : utilisation de suites pseudo-aléatoires et substitution bloc à bloc. Ensuite, nous examinons en détail l'algorithme de substitution bloc à bloc nouvellement normalisé aux U.S.A.

Dans une deuxième partie nous étudions le problème de distribution de clés sur un réseau numérique commuté.

Enfin, nous nous intéressons au problème du chiffrement des données dans un réseau téléinformatique, ainsi qu'à certaines de ses implications techniques et sociales.

SUMMARY

The growing of data transmission sets the problem of protecting these data against possible eavesdropping and/or ill doing.

As a corollary is also set the problem of identifying a terminal or a person wishing to access these data.

The solution is provided by the use of codes protecting the secrecy of data and/or identities.

It is then a matter of cryptography. In the first part of the paper we list 1) the various threats against a data transmission system 2) the two classes of cryptographic codes : a) use of pseudo random sequences and b) block to block substitution.

Then we examine in details the block to block substitution algorithm recently adopted by the US National Bureau of Standards.

In the second part of the paper we study the key distribution problem, over a switched digital network. We conclude by studying data encryption over a packet switching network, from a technical and social standpoint.

COLLOQUE NATIONAL SUR LE TRAITEMENT DU SIGNAL
ET SES APPLICATIONS

NICE du 26 au 30 AVRIL 1977

PROTECTION DU SECRET PAR CHIFFREMENT DANS UN RESEAU PUBLIC A COMMUTATION DE DONNES PAR PAQUETS

GLOSSAIRE

Chiffre : ensemble particulier de conventions pour une correspondance secrète.

Chiffrer : traduire le langage clair en langage chiffré pour assurer le secret des correspondances.

Cryptogramme : texte obtenu après chiffrement ; on l'appelle aussi texte chiffré pour le distinguer du texte clair.

Déchiffrer : traduire en langage clair le langage chiffré en utilisant le moyen de déchiffrement que l'on possède de droit, en particulier la clé.

Décrypter : parvenir au déchiffrement d'un cryptogramme alors que l'on n'en est pas destinataire et que l'on n'en possède pas légitimement la clé.

Systèmes cryptographiques : procédés généraux de chiffrements dont les chiffres ne sont que des cas particuliers.

Cryptographie: mode d'écriture secrète.

Ces définitions correspondent au sens actuellement reconnu des termes du fait de l'évolution du langage. Elles sont tirées du Petit Larousse.

PROTECTION DU SECRET PAR CHIFFREMENT DANS UN RESEAU PUBLIC A COMMUTATION DE DONNEES PAR PAQUETS.

I MENACES SUR UN SYSTEME TELEINFORMATIQUE

Les menaces planant sur un système téléinformatique sont nombreuses et souvent étroitement imbriquées. On peut les préciser par la classification suivante par Feistel (3).

α) Vol d'information par écoute passive - données - mots de passe - modes d'emploi

β) Entrée illégale dans un ordinateur grâce à α)

γ) Injection de données parasites, éventuellement non comprises par l'intrus

δ) Révélation d'information par viol de mémoire principale (liste de mots de passe) ou par vol de mémoires secondaires (disques, bandes,...).

L'introduction du chiffre protège le système contre ces menaces ; mais ne le rend pas invulnérable pour autant ; et on peut reprendre la terminologie des diplomates et des militaires pour exprimer les menaces auxquelles sont exposées les cryptogrammes. Ainsi il y a trois types d'attaques possibles contre un système cryptographique.

1) décrypter le cryptogramme, c'est-à-dire parvenir à en saisir le sens sans en posséder légitimement la clé.

2) brouiller le cryptogramme

3) insérer des données parasites dans le cryptogramme détruisant ainsi l'intégrité d'un message.

Le premier point (décrypter) est une attaque passive, les deux derniers sont des attaques physiques actives. Notons que, sur un réseau commuté, l'attaque active est plus simple à réaliser qu'une attaque passive. Dans un réseau de diffusion, une attaque passive est au contraire plus simple à réaliser.

Ce qui fait la spécificité du chiffrement en téléinformatique, c'est qu'il est très souvent possible, de posséder à la fois un texte en clair et son cryptogramme.

II LA CRYPTOGRAPHIE EN TRANSMISSION DE DONNEES

La protection de l'information dans un système de transmission de données peut être assurée par l'utilisation d'une transformation réversible de l'information elle-même, d'une manière telle que le retour à une forme utilisable ne puisse se faire que par une information de contrôle appelée "clé".

Par système de transmission de données, nous entendons soit une ligne de transmission, soit un réseau numérique de commutation ou de diffusion, soit même l'utilisation de mémoires de masses pour le transfert d'informations ou pour la constitution de banques de données. Dans ce qui suit, nous nous intéresserons essentiellement aux réseaux publics à commutation de données par paquets.

Cependant, il importe de bien réfléchir à toutes les applications possibles des techniques envisagées et donc de définir les marchés potentiels qui justifieraient l'étude et la réalisation de circuits intégrés LSI spécialisés pour les algorithmes envisagés. En effet, le choix d'une solution ne peut se faire sans tenir compte des prix des équipements et donc des possibilités de commercialiser le service correspondant à un coût raisonnable.

Enfin, dans l'intérêt des utilisateurs et des exploitants du réseau, il est souhaitable d'obtenir des normalisations de manière à ce que les communications soient possibles sans intervention du réseau pour passer d'un algorithme de chiffrement à un autre.

III ELEMENTS DE SYSTEMES CRYPTOGRAPHIQUES

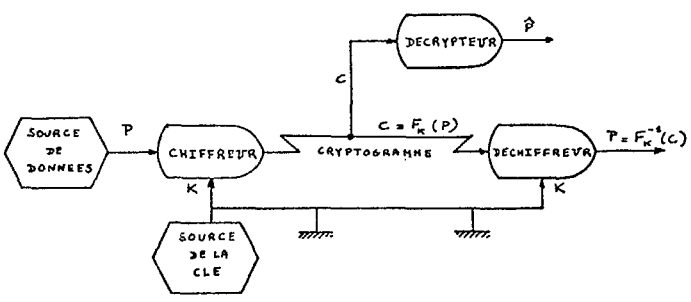


FIGURE 1 : Protection du secret grâce à un canal annexe "sûr".

PROTECTION DU SECRET PAR CHIFFREMENT DANS UN RESEAU PUBLIC A COMMUTATION DE DONNEES PAR PAQUETS.

La figure 1 définit les relations entre les données d'entrée (message en clair), les données transmises (cryptogramme) et les données utilisées (clés) pour contrôler le chiffrement et le déchiffrement. Cette figure définit aussi les rôles respectifs du chiffreur, du déchiffreur et du décrypteur.

Le processus de chiffrement est réversible, c'est-à-dire que par déchiffrement on retrouve le texte original. Par la suite, nous nous intéresserons uniquement aux chiffrements pour lesquels le message et le cryptogramme ont le même nombre de bits.

Deux techniques de base sont susceptibles d'être utilisées pour la protection de l'information numérique :

+ la combinaison bit à bit avec une suite pseudo aléatoire,
+ la substitution bloc à bloc par groupe de n bits.

III - 1 - Suites pseudo aléatoire

L'étude de la génération des nombres pseudo aléatoires fait l'objet d'une abondante littérature. Les travaux de TAUSWORTHE - LEWIS - PAYNE (5) ont abouti à l'étude du polynôme $X^{532} + X^{37} + 1$, irréductible de période $2^{532}-1$.

Un algorithme utilisant ce polynôme permet de générer une suite binaire pseudo aléatoire. Les valeurs initiales des registres de l'algorithme sont obtenues à partir d'une "graine" de 64 bits par une séquence d'initialisation.

La période de la suite binaire obtenue est très grande puisque un calculateur fournissant 10^6 bits par seconde mettrait environ 10^{150} ans à épuiser le cycle !!.

Appelons S_n la suite obtenue par un générateur pseudo aléatoire ayant pour polynôme générateur $X^{532} + X^{37} + 1$.

Le chiffrement consistant en l'addition de la suite S_n au train numérique des messages ; est très solide de par la très longue période de la suite (S_n). Ce système de chiffrement détecte toute tentative d'attaque active de par sa sensibilité à la synchronisation qui est très élevée. Le déchiffrement est très aisé : il consiste en l'addition de la même suite pseudo aléatoire au cryptogramme. Une caractéristique de ce système est l'indépendance des symboles : une erreur sur un bit du cryptogramme n'affecte que le bit correspondant du texte déchiffré.

Ce dernier point peut être un avantage pour les applications dans lesquelles les messages ont un haut degré de redondance avec une forte tolérance aux erreurs. Mais dans les applications de téléinformatique classique, caractérisées par une faible redondance et une faible tolérance aux erreurs, le manque de dépendance entre les symboles est considéré comme un désavantage.

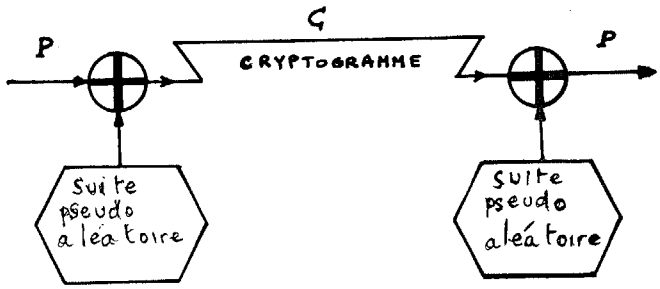


FIGURE 2 : utilisation d'une séquence pseudo aléatoire

III - 2 - Substitutions bloc à bloc

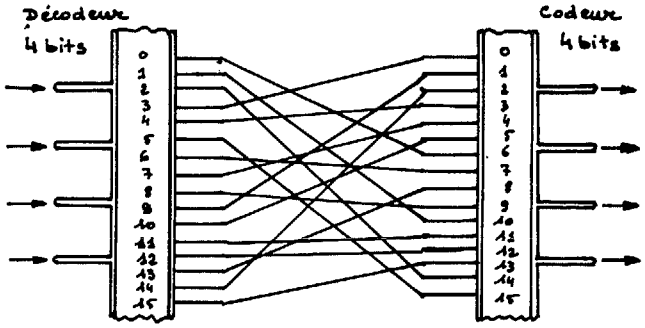


FIGURE 3 : Substitution bloc à bloc pour n = 4

PROTECTION DU SECRET PAR CHIFFREMENT DANS UN RESEAU PUBLIC A COMMUTATION DE DONNEES PAR PAQUETS.

Le circuit SN 74154 décode une entrée sur 4 fils en une sortie parmi 16.

La figure ci-dessus indique ce qu'est la substitution bloc à bloc.

Ainsi il y a exactement 2^n blocs différents de n bits. Et il y a (2^n) ! permutations possibles de cet ensemble de 2^n blocs, qui sont toutes les bijections de n bits sur n bits.

Par exemple, sur la figure 3, il y a 2^4 ! = 16! = 20.922.789.880.000 façons différentes de relier fil à fil les 16 sorties du décodeur et les 16 entrées du codeur.

Un tel système peut fort bien être câblé si n est petit, disons n = 5 ou 6 ; mais un tel système est équivalent à une classique substitution de caractères alphabétiques et est donc notoirement faible. La faiblesse du système n'est pas due à une structure simple, mais plutôt à la petite taille des blocs de bits. Si n est grand, de l'ordre de 100, l'analyse des fréquences de distribution des blocs n'est plus possible, de même que la réalisation d'un décodeur, d'un codeur et de leurs liaisons.

Pour réaliser un algorithme de substitution bloc à bloc, nous allons utiliser la notion de chiffrement multiple, c'est-à-dire effectuer plusieurs chiffrements élémentaires en séquence de sorte que le résultat soit cryptographiquement plus fort qu'aucun des composants.

Ainsi, sur la figure 4, les boites marquées P représentent des permutations de bits et chaque boite S, sous le contrôle de deux bits de la clé, peut opérer une parmi 4 substitution du type schématisé sur la figure 3.

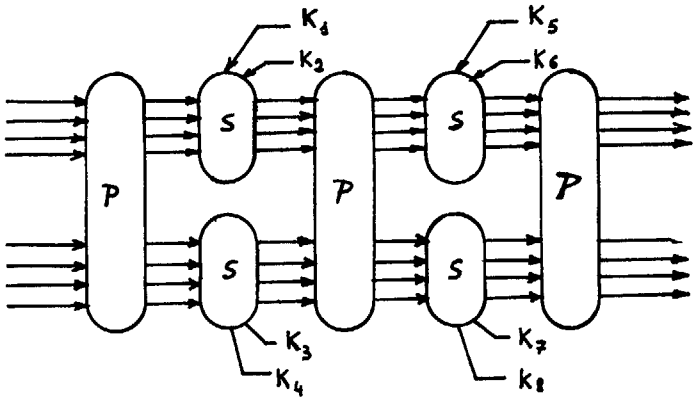


FIGURE 4 : Chiffrement multiple pour n = 8 avec utilisation d'une clé de 8 bits

Le déchiffrement est possible, il suffit de constituer le montage symétrique et d'utiliser les bits de la clé dans l'autre sens.

Les boites S sont telles que chaque état d'entrée parmi les 16 possibles correspond en sortie à un état distant de 2 en moyenne au sens de Hamming. Et de plus, les quatre substitutions possibles sont telles que les quatre états de sortie correspondants à un même état d'entrée sont à leur tour distants de 2 en moyenne au sens de Hamming.

Ainsi l'algorithme de chiffrement de la figure 4 a les propriétés suivantes :

+ la modification d'un bit sur la donnée d'entrée modifiera en moyenne la moitié des bits en sortie.
+ la modification d'un bit de la clé modifiera en moyenne la moitié des n bits de sortie (dans l'exemple proposé en figure 4, les 4 premiers bits de la clé ont plus d'influence que les 4 derniers).

La définition d'une solution par les spécifications des boites S et P dans la figure 4 fournit une famille de 2^8 = 256 fonctions (nombre de clés) parmi les 256 ! façons qu'il y a de relier les sorties d'un décodeur de 8 bits aux 256 entrées d'un codeur sur 8 bits. Mais l'ensemble des octets est constitué de 256 éléments et le procédé se ramène à une substitution alphabétique dont la faiblesse est notoire, car l'analyse de la fréquence d'apparition des octets est

tout à fait faisable et interprêtable.

Si l'on augmente le nombre de bits des blocs considérés, l'analyse des fréquences sera plus difficile et surtout ne sera plus interprêtable. Mais aussi, si l'on travaille avec des blocs de 64 bits, il faudra définir 16 boites S par étage de chiffrement et il faudra de l'ordre de 16 étages pour que le procédé soit solide : les données initiales nécessaires pour définir toutes les boites S sont beaucoup trop volumineuses.

III - 3 - Algorithme en cours de normalisation aux U.S.A.

Il existe une autre manière de spécifier un chiffrement multiple. La procédure consiste à subdiviser le bloc considéré en deux segments égaux, à utiliser un segment comme argument d'une fonction de transformation (qui peut être irréversible) et dont le résultat sert à modifier l'autre segment par une opération réversible. Ceci est illustré par la figure 5.

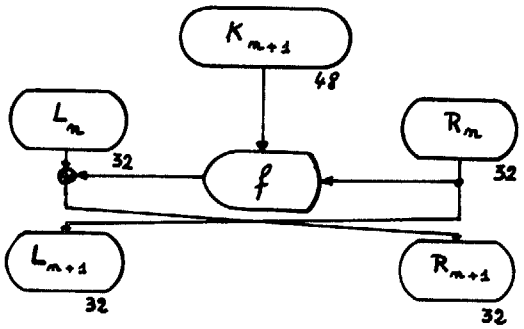


FIGURE 5 : une itération de l'algorithme du chiffre NBS/DES (National Bureau of Standards Data Encryption Standard)

Ainsi : $L_{n+1} = R_n$

$R_{n+1} = L_n \oplus f(R_n, K_{n+1})$

R,L et le résultat de la fonction appartiennent à l'ensemble des blocs de longueur 32. Cet ensemble est muni d'une structure de groupe par l'opération interne $\oplus$. Cette opération peut être l'addition modulo 2^{32} ou le "ou exclusif" bit à bit.

Dans le cas de l'algorithme NBS/DES, l'opération interne est le "ou exclusif" (addition bit à bit modulo 2).

Cette itération de chiffrement est réversible quelle que soit la fonction f ; en effet :

$R_n = L_{n+1}$

$L_n = R_{n+1} \oplus f(L_{n+1}, K_{n+1})$

Il est à remarquer que ce raisonnement peut se généraliser sur plusieurs segments, par exemple :

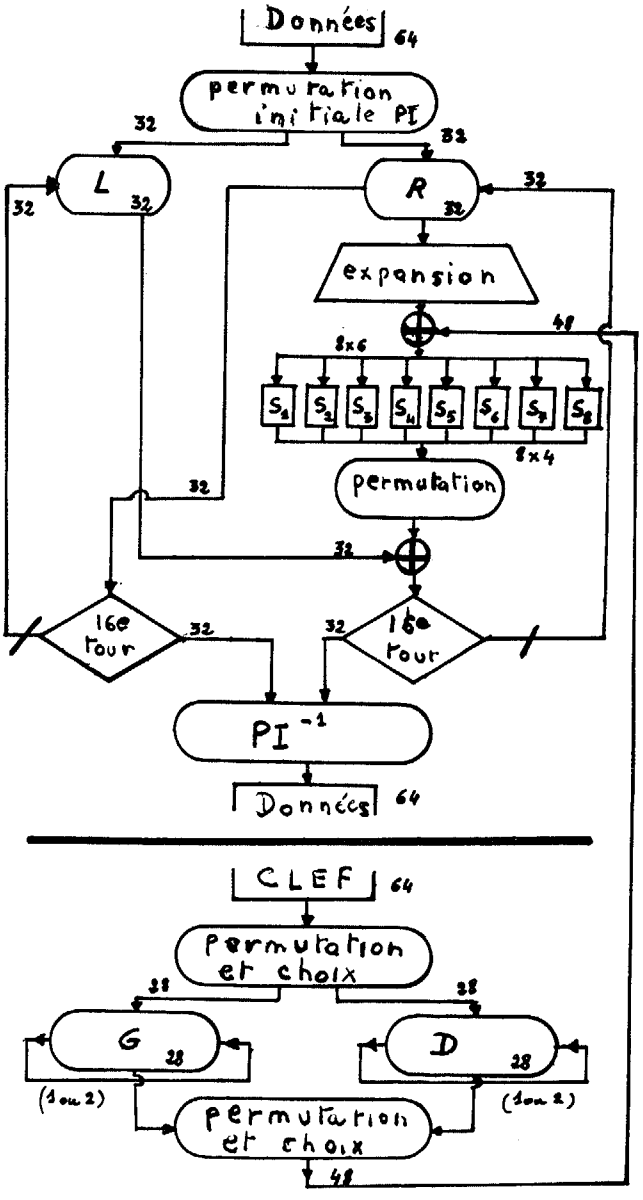
$A_{n+1} = D_n$ $\qquad$ $D_n = A_{n+1}$

$B_{n+1} = A_n \oplus f'(K'_{n+1}, B_n)$ $\qquad$ $C_n = D_{n+1} \oplus f'''(K_{n+1}, A_{n+1})$

$C_{n+1} = B_n \oplus f''(K''_{n+1}, C_n)$ $\qquad$ $B_n = C_{n+1} \oplus f''(K''_{n+1}, C_n)$

$D_{n+1} = C_n \oplus f'''(K'''_{n+1}, D_n)$ $\qquad$ $A_n = B_{n+1} \oplus f'(K'_{n+1}, B_n)$

Mais terminons plutôt la description de l'algorithme NBS/DES par le schéma suivant :



Les bits non utilisés dans la clé servent à vérifier l'imparité pour chaque octet de la clé.

Cet algorithme permet d'obtenir une famille de $2^{56} \simeq 7.10^{16}$ fonctions de substitution de blocs de 64 bits parmis les 2^{64} ! fonctions de ce type. Sa force réside dans le fait qu'une modification d'un seul bit (sur les données ou sur la clé) modifie en moyenne une trentaine de bits sur le cryptogramme.

Deux propriétés de cet algorithme sont des avantages : une synchronisation par blocs de 64 bits est relativement simple à établir ou à retrouver ; une forte interdépendance entre les symboles d'un cryptogramme permet de chainer facilement les blocs successifs.

L'utilisation de cet algorithme nécessite la même clé aux deux extrémités. Ceci pose le difficile problème de l'échange des clés sur le réseau.

Les performances, dans divers cas d'implantation, sont réunies dans la figure ci-dessous.

Implantation	Temps pour chiffrer 64 bits	Débit
Logicielle :		
- grand calculateur	100 µs	640 kb/s
- mini calculateur	50 ms	1,3 kb/s
Matérielle :		
TTL	5µs	13 Mb/s
LSI	50µs	1,3Mb/s

Une réalisation en TTL comprendrait 100 à 150 circuits, contre 4 en LSI (∿ 100 $). Une grande diffusion des circuits LSI ferait tomber leur prix à 20 $, soit 100 FF.

IV STRATEGIES D'UTILISATION DU CHIFFRE SUR UN RESEAU NUMERIQUE COMMUTE

Tout système classique de chiffrement entre deux points suppose l'existence d'une liaison réputée "sure", même de faible débit et à grand délai de transmission, sur laquelle est transmise la clé du code protégeant le secret : sur un réseau public, la liaison sure est difficile à établir, parfois même impossible. En effet, elle consiste souvent en l'envoi de la clé par lettre recommandée, ou bien par porteur spécial. Cette contrainte réduit considérablement la souplesse d'utilisation du réseau : il est souhaitable que deux utilisateurs qui ne se connaissent pas puissent échanger des données chiffrées, sans préavis et sans avoir à gérer et à protéger les $n(\frac{n-1}{2})$ clés permettant de communiquer avec les (n-1) autres utilisateurs du réseau.

L'utilisation des fonctions difficilement inversibles permet d'établir des liaisons chiffrées sans avoir à échanger des clés par une liaison sûre et ceci de deux manières différentes :

- la clé est transmise sur le réseau
- le chiffrement s'effectue sans avoir besoin d'échanger des clés.

IV -1- Système de chiffrement à annuaire (sans échange de clés).

Dans les algorithmes de chiffrement classiques, la transformation de déchiffrement est quasi identique à la transformation de chiffrement. Il s'ensuit que la connaissance de l'une d'elles permet d'en déduire l'autre aisément.

La théorie des fonctions difficilement inversibles permet de définir des couples transformations (E_k, D_k) qui vérifient les propriétés suivantes :

1) pour toute clé k, D_k est la transformation inverse de E_k

2) pour toute clé k, les algorithmes E_k et D_k sont faciles à calculer à partir de k.

3) pour presque toutes les valeurs k, il est pratiquement impossible de calculer D_k à partir de E_k.

Les propriétés 2) et 3) indiquent une méthode d'utilisation de telles transformations pour le chiffrement :

Un utilisateur voulant recevoir des données chiffrées, choisit une clé k, avec laquelle il engendre un couple de transformations (E_k, D_k). Il détruit la clé k, et garde la transformation D secrète. Ceci est d'autant plus facile que D n'a pas à être transmise. La transformation E est mise dans un répertoire public, avec le nom et l'adresse de l'utilisateur. Toute personne voulant communiquer avec l'utilisateur chiffre ses messages avec E. Seul le légitime destinataire pourra les déchiffrer.

IV -2- Transmission des clés sur le réseau

Les fonctions non inversibles permettent l'utilisation d'algorithmes classiques de chiffrement tout en utilisant le réseau pour l'échange des clés.
soient f(x,y) et Ø (x) des fonctions difficilement inversibles ayant la propriété :

$$f(\emptyset(x), y) = f(\emptyset(y), x)$$

si les usagers X et Y veulent déterminer une clé commune et secrète pour communiquer entre eux, ils opèrent de la manière suivante :
X choisit x, qu'il garde secrète et calcule Ø (x), qu'il transmet à Y sur le réseau.
Y opère de même. Il choisit une quantité y, qu'il garde secrète et calcul Ø (y) qu'il communique à X à travers le réseau.
seuls X et Y peuvent déterminer la quantité

$$k = f(\emptyset(x), y) = f(\emptyset(y), x).$$

Cette quantité k leur servira de clé commune. Toute personne interceptant la communication sera en possession de Ø (x) et Ø (y), mais ne pourra déterminer la quantité k.

V LE CHIFFRE DANS LES RESEAUX A COMMUTATION DE DONNEES PAR PAQUETS

L'existence d'un réseau public se traduit pour l'utilisateur par des protocoles standards d'accès au réseau et par une extension considérable des puissances de calcul accessibles.

Sous la pression des concepteurs de réseau et des utilisateurs, les protocoles d'accès et de dialogue avec les ordinateurs seront normalisés et les constructeurs devront respecter les standards adoptés. Ainsi un ordinateur prestataire du service temps partagé ne connaîtra qu'un terminal virtuel, le réseau ou l'utilisateur gérant le terminal réel.

L'architecture téléinformatique des systèmes d'exploitation des ordinateurs sera bouleversée : les différentes fonctions logiques seront de plus en plus séparées pour pouvoir aboutir à une informatique répartie et à une meilleure spécificité des divers constituants. De plus les dialogues entre éléments répartis tendront à se normaliser.

L'usage du chiffre, dans les réseaux à commutation de données par paquets, nous permet de préciser cette évolution en analysant son influence sur les moyens d'accès aux ordinateurs et son rôle dans la protection des transmissions.

V -1 Le chiffre et les moyens d'accès aux ordinateurs

Les données soumises à un organe de traitement doivent être fournies en clair. Un niveau de procédure donné n'a besoin d'interpréter, dans un flot d'information, que les commandes qui lui sont destinées.

Ainsi : les octets de procédure X25 doivent être compris par le noeud de rattachement ; le source d'un programme doit être fourni en clair à un compilateur ; dans un fichier, le corps des articles peut être composé d'un crytogramme de sorte que seul le détenteur de la clé puisse en saisir le sens.

Le chiffre met en évidence la rigueur nécessaire à la conception d'un procédure et le soin à apporter au problème de la transparence , c'est-à-dire à la conservation de l'intégrité du flot de données à un niveau fixé de procédure. Sur les ordinateurs raccordés au réseau public, l'utilisation du chiffre au niveau le plus basique du système, nécessite l'existence d'un canal d'accès "transparent" entre le niveau de procédure visé et le réseau de transmission. Cette obligation coïncide avec l'évolution des moyens d'accès dans les systèmes d'exploitation des ordinateurs. Certains constructeurs envisagent même l'implantation d'un opérateur câblé traitant l'algorithme NBS/DES dans les unités centrales.

Généraliser l'usage du chiffre dans un système téléinformatique, c'est admettre qu'à un niveau de procédure donné, les données transmises puissent être totalement incompréhensibles pour qui n'en possède pas la clé.

V -2- Le chiffre et la protection de la transmission

L'usage du chiffre permet essentiellement de contrer les écoutes passives en rendant insaisissable le sens des messages transmis. En chiffrant les données au niveau des lignes de transmission, on complète utilement la protection physique des sites de commutation ; en chiffrant les communications, les informations sont rendues inaccessibles au personnel mettant en oeuvre le réseau.

Cependant si certaines données sont très sensibles au secret, certains messages sont très sensibles à l'intégrité : la protection du secret empêche partiellement les modifications intelligentes des messages transmis, mais l'usage du chiffre permet également d'assurer la validité des messages et donc de contrer d'éventuelles attaques actives.

Une indication horaire précise jointe avant chiffrement, permet de limiter la période de validité du cryptogramme et de contrer un éventuel rejeu. Dans le cas d'une substitution bloc à bloc, le chainage des blocs avant chiffrement permet de vérifier l'intégrité du message transmis.

Le chiffre apparait comme une des conditions au développement harmonieux d'un service public de transmission de données. La sécurité offerte par le chiffre est un phénomène essentiellement probabiliste. Le risque de décryptage, même très faible, existe toujours ; il peut être réduit par un surchiffrement et est de toute façon bien plus faible que la probabilité de vol ou de perte de courrier postal.

VI LE CHIFFRE ET LA PROTECTION DES LIBERTES

Traditionnellement le chiffrement correspondant à la protection des informations que l'on ne désire pas divulguer, c'est-à-dire celles dont la connaissance par un tiers entrainerait des conséquences fâcheuses, mêmes dramatiques : il faut donc assurer le secret, tel est le cas, par exemple, des informations concernant la défense nationale.

Mais il existe une autre catégorie d'informations : celles dont la connaissance en elle-même n'est pas importante, mais dont le regroupement avec toutes les autres de la même catégorie donne un pouvoir certain. Tel est le cas, par exemple, des informations concernant un même individu. La protection des libertés individuelles réside dans l'impossibilité, physique ou légale, de regrouper les divers fichiers existants et concernant les individus.

L'existence d'un réseau public offre de vastes possibilités pour un observateur indélicat. Il peut voler les informations transitant sur le réseau, d'où la possibilité de constituer des fichiers de données ou de récupérer des procédures d'accès aux diverses bases de données. Il pourrait ainsi obtenir toutes les informations concernant tel ou tel individu, pourvues qu'elles transitent par le réseau ou qu'elles soient accessibles à partir du réseau.

Pour contrecarrer ces manipulations frauduleuses, le chiffrement sera nécessaire et fera échec à l'observateur indélicat.

Le chiffre est donc ainsi un moyen de protéger des informations non sensibles en elles-mêmes, mais dont le regroupement avec d'autres doit être empêché. Le chiffre apparaît ainsi comme un moyen, mais ce n'est pas le seul, de protéger les libertés individuelles.

VII BIBLIOGRAPHIE

(1) G.J. CHAITIN - Information theoretical computational complexity IEEE-IT-20 N°1 January 1974

(2) W.DIFFIE,M.E. HELLMAN - Nex directions in cryptography IEEE-IT-22-November 1976

(3) H. FEISTEL, W.A. NOTZ,J.L. SMITH - Some cryptographic techniques for machine to machine data communications. Proccedings IEEE Vol. 63 N° 11, November 1975

(4) E. GUDES, H.S KOCH, F.A. STAHL - The application of cryptography for data base security. N.C.C. 1976

(5) T.G. LEWIS, W.H. PAYNE - Generalized feedback shift register Pseudo Random Algorithm. Journal A.C.M. Vol. 20 n° 3 July 1973

(6) S.C. POHLIG, M.E. HELLMAN - An improved algorithm for computing logarithms over GF (p) and its cryptographic significance - Preprint

(7) P.E. SCHMID - Review of ciphering methods to achieve communication in data transmission networks

(8) D.J. SYKES - Protecting data by encryption Datamation, August 1976

(9) D.J. TORRIERI - Cryptographic digital communication IEEE transactions on Aerospace Vol. AES12-N°1 January 1976

(10) WIDMER - Message authentication, a special identification requirement in one way digital transmission

(11) Encryption algorithm for computer data protection. U.S. Federal Register. Vol 40 n° 52 March 17, 1975.

ANNEXE - FONCTIONS DIFFICILEMENT INVERSIBLES

La notion de fonction difficilement inversible est une notion relative à l'état actuel des connaissances et à l'état de la puissance de calcul disponible.

Une fonction f d'un ensemble A dans un ensemble B est dite difficilement inversible si, étant donné y B, la détermination de x A tel que $f(x)=y$ nécessite au moins 10^{20} opérations, et ceci par le meilleur algorithme connu.

Considérons le couple de fonctions :

$$x \rightarrow y = \nabla^x \text{ modulo } p$$

$$y \rightarrow x = \log_{\nabla} y \text{ modulo } p$$

ce sont les fonctions exponentielle et logarithme sur le corps fini CG (p), p est un nombre premier et ∇ un élement primitif de CG (p). C'est ce couple de fonctions inverses l'une de l'autre qui présente la plus grande dissymétrie de calculabilité. Considérons l'exponentielle modulo p. Le calcul de ∇^x peut se faire en 2 $[\log_2 p]$ opérations, avec seulement 3 mots de mémoire de $[\log_2 p]$ bits chacun. ([A] dénote la partie entière par excès de A.)

Le calcul des logarithmes modulo p est beaucoup plus difficile. Soit la décomposition ordonnée de p-1 en facteurs premiers :

$p-1 = p_1^{n1} \ldots\ldots p_k^{nk}$

Théorème 1 : les logarithmes modulo p sont calculables en $O(\Sigma n_i\ p_i)$ pas de calcul en utilisant O(k) mot de mémoire de longueur $\log_2 p$.

Théorème 2 : Les logarithmes modulo p sont calculables en $O(\Sigma n_i\ \sqrt{p_i}\ \log_2 p_i)$ pas de calcul en utilisant $O(k+\sqrt{p}k)$ mots de mémoire de longueur $\log_2 p$.

Théorème 3 : Les logarithmes modulo p sont calculables en $O(\Sigma_{pi})$ mots de mémoire de longueur $\log_2 p$.

Chacun des trois théorèmes représente un compromis entre le temps et l'espace pour le calcul Si tous les facteurs premiers de p-1 ne sont pas trop grands, alors les théorèmes sont très semblables.

Soit $p = 2p' + 1$, où p' est premier ; forme qui rend le calcul le plus laborieux. Le théorème 2 représente un compromis entre temps et espace : O $(\sqrt{p})$ pas de calculs et O $(\sqrt{p})$bits de mémoire. Si p est de l'ordre de 2^{400}, $\sqrt{p}$ est de l'ordre de 10^{60}. Cela revient à dire que cent milliards de processeurs effectuant chacun cent milliards d'opérations par seconde mettraient 10^{30} ans à calculer un logarithme modulo p. S'il ne fallait qu'une molécule par bit de mémoire, il faudrait plus de 10^{38} moles de matière pour mener à bien ce calcul : la masse du système solaire n'y suffirait pas.

L'exponentielle modulo p est calculable en 800 multiplications modulo p et quelques mots de 400 bits pour les nombres de l'ordre de 2^{400}.