ASSOCIATION des RÉSERVISTES du CHIFFRE et de la SÉCURITÉ de L'INFORMATION

Histoire de la machine MYOSOTIS

Gilles Ruggiu

Numéro hors série
Juillet 2003

ASSOCIATION des RÉSERVISTES du CHIFFRE et de la SÉCURITÉ de L'INFORMATION

Histoire de la machine MYOSOTIS

Gilles Ruggiu

Numéro hors série
Juillet 2003

Histoire de la machine

MYOSOTIS

par

Gilles Ruggiu

Juillet 2003

À la mémoire

de

Monsieur MULLER

Remerciements

Cette histoire a pu être réalisée grâce aux renseignements que m'ont transmis :

- Jean-Pierre VASSEUR ;
- Xavier AMEIL ;
- Marc DUMAIRE ;
- André CATTIEUW ;
- Louis RIBADEAU DUMAS.

Ils m'ont aussi remis des documents que j'ai quelquefois utilisés tels quels.

Qu'ils en soient tous chaleureusement remerciés, ainsi que Christian FABRE et Georges ANDRÉ qui m'ont donné oralement plusieurs informations relatives aux concours OTAN et national.

Jacques RIETHMÜLLER et Joël LEBIDOIS m'ont aussi fourni divers renseignements et fait quelques commentaires sur une version préliminaire de cet historique. Je leur en suis très reconnaissant.

Je remercie également François-Joseph RUGGIU, professeur d'histoire à l'Université de Bordeaux-III, qui a bien voulu relire tout le manuscrit.

Je n'oublie pas, non plus, André MULLER qui m'avait fortement encouragé à réaliser cet historique.

Mais toutes les erreurs et omissions qui subsistent sont de mon seul fait.

Gilles RUGGIU.

SOMMAIRE

INTRODUCTION

L'histoire de la cryptographie est faite d'épisodes brillants mais aussi de périodes de décadence dont la France n'est pas exempte. Les années qui ont suivi la Deuxième Guerre mondiale correspondent à un affaiblissement important et une inadéquation des moyens de chiffrement gouvernementaux. La plupart de ces moyens étaient en effet issus de la guerre et sont devenus par la suite particulièrement inadaptés, en particulier avec le développement des transmissions par téléimprimeurs.

C'est l'opération de Suez en 1956 qui en fut le révélateur et qui décida le gouvernement de l'époque à se doter de moyens modernes. C'est ainsi que fut organisé un concours entre différents industriels français sous l'égide des administrations concernées par cette technique. Il faut reconnaître que cet état de fait n'était pas propre à la France. Au même moment, la plupart des autres nations occidentales firent un constat similaire : leurs moyens de chiffrement s'avéraient de moins en moins appropriés aux besoins modernes de communication. C'est pourquoi l'OTAN lança un concours analogue.

C'est dans ce contexte que se déroula le projet Myosotis qui marqua le renouveau du Chiffre en France. Il fut d'une importance particulière pour la cryptographie française car il eut pour conséquences de :

- doter la France d'une industrie du Chiffre capable de rivaliser avec les autres grandes puissances, et de satisfaire la plupart des besoins gouvernementaux ;
- définir, sous l'impulsion du Service Technique Central des Chiffres (STCCh), la doctrine du Chiffre en matière gouvernementale pour la conception, l'évaluation et l'emploi des moyens de cryptologie de l'État ;
- constituer une véritable école française du Chiffre, qui perdure encore même si les structures actuelles sont bien différentes de celles de cette époque.

Par sa conception, qui s'appuyait sur la meilleure approximation possible du secret parfait, on peut dire que la machine

Myosotis reste une des meilleures machines à chiffrer jamais réalisées, compte tenu de son domaine d'emploi et des performances exigées à l'époque.

Cette histoire retrace les principaux événements et faits qui ont marqué le projet Myosotis, y compris quelques mésaventures ou péripéties qui éclairent certains aspects concrets de la sécurité de l'information.

L'histoire de Myosotis et de ses suites est divisée en quatre parties et une conclusion. La première présente les administrations et les industriels qui ont été concernés par ce projet. On donne aussi un état des moyens de chiffrement français à cette époque. La deuxième partie retrace les circonstances des concours français et OTAN, ainsi que les considérations qui conduisirent au choix final. La troisième décrit la mise en place de l'industrie du Chiffre en France. La quatrième partie évoque les travaux qui suivirent ceux de Myosotis et comment le Chiffre civil non gouvernemental fut abordé en France à la fin des années soixante-dix. La conclusion tente de faire un point rapide sur la situation actuelle.

Quatre annexes complètent cet historique.

La première définit les grands principes de la cryptographie à travers son histoire. En effet, il nous a semblé que, pour comprendre le sujet, il était indispensable de présenter, même sommairement, quelques éléments concernant les principes de base de la cryptographie et de la théorie des systèmes secrets. On pourra s'y référer pour retrouver la définition des principaux termes techniques relatifs à la cryptographie (les termes définis sont imprimés en caractères gras). Nous y donnons aussi quelques indications historiques sur le développement de ces principes.

La deuxième annexe décrit le fonctionnement de la machine à chiffrer Myosotis.

La troisième contient deux textes. Le premier, de Xavier AMEIL, expose deux anecdotes relatives à Myosotis ; le second texte, du colonel CATTIEUW, est un commentaire sur la première de ces anecdotes. Ces textes illustrent la nécessité impérieuse

d'une bonne application des procédures de sécurité. Ils ont été repris du numéro 29 du *Bulletin de l'ARCSI* (année 2001).

La quatrième annexe aborde une question conceptuellement difficile, mais centrale pour la cryptographie, celle de la notion d'aléa. L'approche qui est présentée nous paraît correspondre le mieux à l'esprit de la cryptographie.

Enfin, quelques photographies complètent ce dossier. Les trois premières présentent quelques-uns des acteurs du projet Myosotis. Les quatre suivantes montrent comment se présentait physiquement un ensemble de chiffrement Myosotis ; la dernière photo est une image de l'aléa produit par Myosotis.

PREMIÈRE PARTIE

L'ÉTAT DE LA CRYPTOGRAPHIE EN FRANCE AVANT MYOSOTIS

I.1. – INTRODUCTION.

À l'heure actuelle, toute personne portant un intérêt à l'électronique en général, et aux télécommunications en particulier, trouve normal que la CSF (Compagnie générale de télégraphie Sans Fil, fondée en 1918 par Émile GIRARDEAU) dont le cœur de métier était les télécommunications se soit occupée des machines électroniques de chiffrement. Pourtant, une telle décision n'était pas du tout évidente au début des années soixante, lorsque l'on a parlé pour la première fois en France de la possibilité de réaliser de telles machines.

Il faut donc rappeler quelle était, dans notre pays, la situation des télécommunications à cette époque. On examinera en premier lieu le rôle et le fonctionnement des services officiels, tant civils que militaires, puis la position de la CSF.

Pour expliquer les décisions des autorités gouvernementales qui ont conduit à la fabrication de moyens de chiffrement modernes, nous présentons d'abord un bref panorama des matériels utilisés au sein des administrations françaises dans les années cinquante et des problèmes que posait leur emploi. Ces décisions ainsi que celles des pays de l'OTAN ont débouché sur l'organisation d'un concours interne en France et d'un concours international entre plusieurs pays de l'OTAN, qui se sont déroulés simultanément. Ces concours ont vu la participation de plusieurs organismes étatiques et plusieurs industriels français. C'est dans ce contexte, que s'est effectuée la mise au point de la machine Myosotis. C'est pourquoi nous présentons aussi les travaux des machines concurrentes de Myosotis et des industriels français intéressés par la fabrication de machines à chiffrer.

I.2. – LES ADMINISTRATIONS CIVILES.

À cette époque, une administration civile, qu'on appelait alors les PTT (Postes, Télégraphes et Téléphones) détenait le monopole des Télécommunications. Son problème était d'assurer la discrétion des liaisons téléphoniques dans ce que l'on appellerait aujourd'hui un souci de protection de la vie privée. Elle se souciait assez peu du secret des communications, probablement parce que celui-ci était en principe garanti par la Loi (mais la loi ne prévoyait aucune disposition technique permettant d'obtenir ce secret).

Elle avait toutefois adopté pour les liaisons radio-téléphoniques un mécanisme de protection consistant à renverser la bande de fréquences du signal de la parole (250 à 2 750 Hz), via un modulateur à 3 000 Hz : après filtrage, la modulation était inversée autour de la fréquence centrale 1 500 Hz. C'est ce que l'on appelait le « secret international ». En cas d'interception, ce dispositif rendait la conversation inaudible (ou plutôt difficile à comprendre). Mais ce système était très facilement décryptable. Il suffisait de renverser à nouveau la bande. En réalité, il n'y avait pas de secret car il n'y avait pas de clé secrète.

Ce système avait donc été ensuite rendu plus compliqué en divisant cette bande en cinq parties à peu près égales et en modifiant l'ordre dans lequel se trouvaient ces cinq morceaux de bande (la largeur des morceaux de bande était autour de 550 Hz). En outre chaque morceau de bande pouvait aussi être inversé. C'était le « secret à découpage de bande ».

Cette transformation du spectre était réalisée, de façon mécanique, au même instant aux deux extrémités de la ligne de transmission. La combinaison qui, à chaque instant, définissait ces permutations et inversions était changée périodiquement (typiquement toutes les vingt secondes) par un système mécanique à base de cames qu'un moteur électrique faisait tourner. Un seul dispositif de secret suffisait pour l'ensemble des deux voies de transmission, grâce au mécanisme de blocage des voies assurant l'alternat dans chaque sens.

Il fallait assurer un parfait synchronisme entre le moteur de l'émetteur et celui du récepteur. La vitesse des moteurs était contrôlée par un diapason vibrant à 300 Hz en enceinte thermostatique. Ceci suffisait pour assurer le maintien du synchronisme pendant vingt-quatre heures après une mise en phase qui était effectuée au début de la journée.

Ce système, qui avait été conçu par la compagnie américaine *Western Electric Company,* permettait de choisir à chaque changement une combinaison parmi six : c'est ce qui constituait le secret. Ce dispositif était complexe et relativement lourd à mettre à œuvre. Cependant le secret était considéré comme faible car une analyse de la continuité des bandes de fréquences permet en principe de reconstituer le signal clair, au besoin en faisant quelques essais si des incertitudes de continuité apparaissent. Mais les périodes de silence, qui sont nombreuses dans une conversation, gênaient considérablement cette reconstruction et le décryptement, en réalité, n'était pas du tout facile avec les moyens plutôt limités de l'époque.

Par ailleurs, au plan interministériel, il existait un service qui dépendait directement du Premier ministre (par le canal du Secrétariat général du gouvernement) : le Service Technique Central des Chiffres (STCCh) [1]. Créé en 1951, sa mission était de promouvoir le Chiffre français. Il supervisait au point de vue technique tout ce qui se faisait en matière de chiffrement dans toutes les administrations civiles et militaires et coordonnait leurs services du Chiffre.

Ce service avait été créé en même temps que la Commission Interministérielle des Chiffres (CIC), pour traiter d'une façon coordonnée et au niveau interministériel des problèmes du Chiffre. Le chef de ce service était André MULLER, à l'époque commandant de gendarmerie, mais que tout le monde appelait M. MULLER ; il sera nommé général de gendarmerie en 1974.

---

[1] Pour plus de précisions concernant la création et l'historique de cette organisation, on pourra se reporter aux articles de L. RIBADEAU DUMAS parus dans les numéros 5 (1977) et 12 (1984) du *Bulletin de l'ARCSI* et à celui de A. CATTIEUW, paru dans le numéro 26 (1998-1999) de ce même bulletin.

Ce service, structure légère d'impulsion et de coordination, disposait de moyens très réduits, puisque à l'origine, il n'y avait qu'un chef de service et deux adjoints. Il n'avait pas de budget pour financer des études, ni de moyens matériels modernes, à part un atelier de fabrication de bandes perforées aléatoires, créé en 1958 et installé dans la caserne du Mont-Valérien. Cet atelier avait la charge d'assurer l'approvisionnement en bandes-clés « une fois » des départements ministériels qui ne voulaient ou ne pouvaient produire ces clés eux-mêmes. Le STCCh était donc assez démuni face aux nouvelles technologies électroniques et informatiques qui allaient se développer [2].

Le STCCh assurait aussi un cours par correspondance permettant d'obtenir le certificat d'études cryptographiques, certificat qu'il fallait posséder pour obtenir le grade de chiffreur en chef dans les administrations, et le certificat technique pour les armées de Terre et de l'Air.

Enfin, il avait été créé, sur l'initiative du général GUÉRIN, au sein du comité d'action scientifique de Défense nationale, un Centre d'Études Cryptographiques Supérieures (CECS) pour la formation de chiffreurs de haut niveau. Le STCCh y participait ainsi que des professeurs d'université qui deviendront d'ailleurs pour la plupart des conseillers scientifiques du STCCh. Le CECS sera rattaché au STCCh en 1962.

C'est en septembre 1962, que les lieutenants André CATTIEUW et Georges ANDRÉ, détachés de l'armée de l'Air dans le cadre du projet Violette (dont il est question au paragraphe II.1 de la deuxième partie), arrivent au STCCh et où

---

[2] André MULLER entretenait d'excellentes relations avec le service homologue allemand : le *Zentralstelle für das Chiffrierwesen (ZfCh)*. En particulier il avait de très bons rapports avec le patron de ce service, le docteur GOING. À la différence du STCCh, ce service allemand avait des capacités de développement et de réalisation de matériels cryptographiques (fabriqués ensuite par des industriels comme Siemens ou Telefunken), et avait donc des compétences industrielles que ne possédait pas le STCCh. Or l'emploi des nouveaux dispositifs électroniques requérait des connaissances physiques nouvelles. Par des échanges avec ce service et ses discussions avec le docteur GOING, André MULLER pouvait se forger une opinion sur la technologie.

ils font leurs premières armes en cryptographie. Ils constituent avec les capitaines Michel SILVESTRE et Jean-Paul FABREGUETTES, déjà en poste au STCCh, l'équipe chargée de suivre les travaux d'évaluation des trois machines en piste pour le concours national. SILVESTRE était plus spécialement chargé de la machine Ulysse, CATTIEUW de Myosotis et ANDRÉ de Violette. Mais CATTIEUW étant de l'armée de l'Air devait aussi s'occuper de Violette. Cette équipe était pilotée par LLOPIS, du ministère de l'Intérieur.

Georges ANDRÉ quitta le STCCh en juin 1964 pour rejoindre la base aérienne 134, au bureau Chiffre des transmissions de l'armée de l'Air à Versailles où il retrouva le commandant Christian FABRE. Ce dernier, après avoir obtenu son diplôme du Centre d'études cryptographiques supérieures en 1962, était l'adjoint du chef du bureau Chiffre et avait participé l'année précédente aux opérations aériennes du concours OTAN pour la machine Myosotis.

Rapidement, André CATTIEUW se révéla éminent cryptologue, et sa collaboration au STCCh dépassa les limites strictes du projet Violette. Il resta au STCCh, où il devint très tôt l'adjoint de MULLER, et lui succéda à la tête du service en 1976.

Le STCCh assurait le secrétariat de la sous-commission « Cryptologie » (cette appellation n'était pas officielle) de la Commission interministérielle des Chiffres, dont il était l'organe permanent d'étude et de conseil. Cette sous-commission, sur le rapport du STCCh, donnait un avis sur la valeur cryptologique et sur l'emploi des moyens de cryptologie de l'État destinés à la protection des informations classifiées des administrations civiles et militaires. Cette sous-commission devait disparaître en 1986, lors de la mise en place de la Délégation Interministérielle de la Sécurité des Systèmes d'Information (DISSI, cf. le paragraphe IV.5).

C'est dans cette sous-commission que l'on trouvera des acteurs importants de l'aventure Myosotis : RIBADEAU DUMAS, GAUBERT, LLOPIS, RABAUD...

Il est à remarquer que l'administration des PTT n'était pas représentée à la Commission Interministérielle des Chiffres (CIC). En fait cette administration affichait une certaine indifférence, voire une certaine méfiance, envers les actions de ces commissions et du STCCh, considérant sans doute que ses systèmes de secret n'étaient pas à proprement parler des machines cryptographiques. Pourtant, comme nous l'expliquerons au début de la deuxième partie, c'est à l'occasion de travaux de modernisation de ces systèmes que prit corps le projet Myosotis.

I.3. – LES ADMINISTRATIONS MILITAIRES.

En France, chaque armée avait son propre service d'études dans le domaine des télécommunications, à savoir :

- la SEFT (Service d'Études et de Fabrication des Transmissions) pour l'armée de Terre ;
- le STTA (Service Technique des Télécommunications de l'Air) pour l'armée de l'Air ;
- le STTM (Service Technique des Transmissions de la Marine) pour la Marine.

Enfin, l'État-major des Armées avait un organisme de concertation : la Commission centrale des transmissions, où se prenaient les grandes décisions communes aux Armées, qui devint ensuite la Commission Interarmées des Transmissions, de l'Électronique et du Chiffre (CITEC). Cette commission avait une sous-commission « Chiffre », spécifique aux Armées, et distincte de la CIC, qui, elle, regroupait, l'ensemble des départements civils et militaires (Affaires étrangères, Intérieur, Colonies, SGDN, SDECE, Air, Terre, Mer, Gendarmerie...).

La direction de l'exploitation du Chiffre était assurée par les services « Chiffre » de chaque armée. Pour l'armée de l'Air et la Marine, ces services étaient rattachés aux transmissions. Pour l'armée de Terre, ce rattachement fut décidé en 1956 : le général MARTY, directeur central des transmissions, fit appel au colonel Louis RIBADEAU DUMAS, alors en poste à Fontainebleau, pour prendre la direction du bureau Chiffre de

la Direction centrale des transmissions, installé aux Invalides. Il avait comme adjoint le commandant SEYER. Félix RABAUD, capitaine à cette époque, faisait partie de ce bureau. Au titre de ses nouvelles fonctions, RIBADEAU DUMAS devint membre de la sous-commission « Cryptologie » dont la présidence fut assurée par l'ingénieur en chef des Télécommunications Maurice OLLIER jusqu'en 1962.

RIBADEAU DUMAS quittera cette sous-commission en 1959 lorsqu'il sera nommé à Oran. Il reviendra d'Algérie en 1962, comme chef de la division « Transmissions et Chiffre » de l'État-major des Armées (situé boulevard Saint-Germain), et présidera la Commission centrale des transmissions.

Il n'y avait pas de compétition entre les trois armées pour étudier et faire réaliser un matériel spécifique d'une armée, mais des difficultés pouvaient apparaître lorsqu'il s'agissait de composants ou de matériels intéressant les trois armées. C'était, en particulier, le cas de l'informatique qui était naissante. Aussi, en 1961, la Délégation Ministérielle de l'Armement (DMA, qui devint plus tard la DGA) a-t-elle créé un Service Central des Télécommunications et de l'Informatique (SCTI). Ce service fut chargé des études et des réalisations communes aux Armées. Plus tard, la SEFT lui sera rattachée.

Le premier patron du SCTI fut l'ingénieur général LACOSTE, qui eut pour adjoint l'ingénieur général CASAL.

I.4. – L'ORGANISATION DE LA CSF.

Le groupe de la CSF comprenait en dehors des établissements purement CSF (rue du Maroc à Paris, Malakoff, Puteaux...), l'ancienne SFR (Levallois, Cholet) et différentes filiales (tant en France qu'à l'étranger) qui étaient étroitement associées aux directions fonctionnelles de la CSF, voire intégrées aux groupements opérationnels correspondants.

La CSF comptait à cette époque environ vingt mille personnes et entretenait un ensemble de laboratoires de recherches de deux mille personnes, ingénieurs et techniciens. Cet

ensemble, appelé collectivement laboratoire de recherches, était dirigé par Maurice PONTE. Celui-ci succéda en 1960 à Robert TABOUIS comme président-directeur général de la société.

En ce qui concerne les directions opérationnelles, on pouvait considérer que le groupe CSF comprenait quatre grandes divisions :

- une division « Matériels professionnels, militaires et civils » (Malakoff, Levallois, Cholet, Issy-les-Moulineaux) ; les études de base, par domaine, se faisaient rue du Maroc, à Levallois et au Département de Physique Appliqué (DPA) installé à Corbeville (Orsay) ;
- une division « Tubes électroniques » (Levallois) avec des laboratoires d'études rue du Maroc et à Levallois, et son important centre de recherches de Corbeville : Centre de Physique Électronique et Corpusculaire (CEPEC) ;
- une division « Matériels grand public », dérivés de l'électronique ou des techniques associées ; elle est composée essentiellement de filiales : AREL-CLARVILLE, CAMECA, SAIP-VEGA, LTI, MOP... ;
- une division « Matériaux et composants » : son laboratoire d'études était à Puteaux au Centre de recherches physico-chimiques de la CSF (CRPC) et sa principale usine de fabrication de semi-conducteurs était à Saint-Égrève. Elle comprenait plusieurs filiales françaises et italiennes, intégrées au groupement « Composants » (LCC, CICE, OREGA, COFELEC, COSEM devenue plus tard SESCOSEM...). Le directeur administratif et commercial de RPC était Xavier AMEIL, qui précisons-le pour la suite, entretenait d'excellents rapports avec l'ingénieur général CASAL, du SCTI.

Les différents laboratoires de RPC étudiaient de nouveaux composants, notamment ceux à semi-conducteurs. Les travaux portaient sur les deux filières technologiques de l'époque, celle au germanium comme celle au silicium. Mais la technologie au silicium était encore expérimentale. Ces composants étaient développés dans l'usine de Saint-Égrève.

L'un de ces laboratoires avait pour objectif de promouvoir l'utilisation de ces composants à semi-conducteurs. C'est là que Jean-Pierre VASSEUR, qui connaissait parfaitement leurs possibilités, disposait d'une équipe orientée dans ce sens, capable de concevoir des équipements de mesure et de nouveaux matériels utilisant ces composants.

Sur le plan commercial métropolitain, il existait pour la division « Matériels professionnels » des commerciaux affectés respectivement à chacune des trois armées et des commerciaux pour les administrations civiles (PTT, Radiodiffusion, Aviation civile, clients divers).

Les divisions « Tubes électroniques » et « Composants » avaient leurs commerciaux propres. Le service commercial de Puteaux, dirigé par Xavier AMEIL, avait la responsabilité de toutes les relations commerciales avec les administrations pour toute la division « Composants ».

1.5. – LES MATÉRIELS CRYPTOLOGIQUES MILITAIRES FRANÇAIS DES ANNÉES CINQUANTE.

À cette époque, les machines du temps de guerre C36, M209, B211, conçues en 1935-1936 par le constructeur suédois Boris HAGELIN et qui avaient été adoptées par la France, étaient toujours en service dans les armées françaises [3]. Elles avaient été modifiées, ainsi que leurs conditions d'emploi, pour en améliorer la valeur cryptographique. Une machine électromécanique, la CX52, dont la France avait acheté la licence de fabrication était aussi utilisée. Elle était de conception plus récente et on pouvait lui adjoindre un clavier.

On disposait en outre des machines KL-7 de l'OTAN, dont la conception était différente de la famille des machines HAGELIN et rappelait la machine à chiffrer Enigma qui avait été utilisée par les Allemands pendant la dernière guerre. La KL-7 était une machine à rotors (voir plus loin) comme l'Enigma. De la

[3] Voir l'article de A. CATTIEUW, « Rétrospective de la cryptologie de 1928 à nos jours », *Bulletin de l'ARCSI*, n° 26, pp. 25-47.

taille d'une grosse machine à écrire (25 litres environ), elle possédait sept rotors dont deux étaient en réserve pour les rechanges. Les cinq rotors actifs avançaient tous à chaque lettre chiffrée (contrairement à l'Enigma où un seul rotor avançait d'une lettre à la fois). Son circuit électrique comprenait quatre tubes électroniques blindés : trois thyratrons et une triode. Cependant son clavier était très dur et on pouvait à peine taper plus d'une lettre par seconde.

Cette machine présentait de très forts rayonnements compromettants aussi bien électromagnétiques qu'acoustiques ; elle était aussi extrêmement bruyante. Elle ne satisfaisait pas du tout les critères TEMPEST (cf. le paragraphe II.4) et, bien que portable, elle n'était exploitable que dans des locaux spécialement aménagés. Il existait aussi un modèle fonctionnant sur batterie, beaucoup moins bruyant et dont les fuites électromagnétiques étaient plus faibles [4].

Ces matériels constituaient les seuls moyens mécaniques ou électromécaniques disponibles. Ils fonctionnaient uniquement en mode hors ligne.

Toutes ces machines sont basées sur un ensemble de rotors, sortes de roues munies de dents ou d'ergots, et de barrettes, munies de tétons, qui s'entraînent mutuellement dans un mouvement plus ou moins régulier et produisent pour chaque lettre claire un alphabet de chiffrement différent. Elles mécanisent un procédé de substitution à double clé. Le calcul du crypto d'une lettre est défini par le carré de VIGENÈRE (cf. annexe I, paragraphe 6) : ce carré est constitué des vingt-six alphabets obtenus à partir de l'alphabet normal par un décalage de une lettre, de deux lettres, etc., jusqu'à vingt-six lettres de décalages, comme avec le chiffre de Jules CÉSAR (voir annexe I, paragraphe 2). Pour simplifier la mécanique, les opérations de chiffrement et de déchiffrement sont identiques, c'est-à-dire que chacune de ces opérations est sa propre inverse (c'est la méthode de calcul appelée « variante allemande »).

---

[4] Malgré ses défauts la KL-7 est restée en service au sein de l'OTAN jusqu'en 1985, quand fut arrêté l'espion WALKER dont nous parlons à la note 12 du paragraphe II.5.

La suite des substitutions poly-alphabétiques qu'engendrent ces machines est cependant périodique (puisque le nombre d'états de toutes ces machines est fini, ils se répètent nécessairement) et la période est plus ou moins longue selon le nombre de roues et la loi d'avance des roues : la M209 (aussi appelée Converter) a une des plus grandes périodes avec plus de 10^8 pas (exactement $26\times25\times23\times21\times19\times17 = 101405850$). Toutefois la CX52 était une machine sensiblement plus complexe que les autres, car ses roues avançaient irrégulièrement.

Quelques années après la guerre de 39-45, un premier projet de construction d'une machine électromécanique « moderne » avait été entrepris et étudié au CNET sous l'égide d'un groupe de travail de la CIC : l'amiral HENNEQUIN avait conçu une nouvelle structure de machine à chiffrer basée sur l'emploi de sélecteurs téléphoniques (et non plus de roues dentées), ce qui permettait de mettre en œuvre une logique beaucoup plus riche et souple ; elle devait en principe permettre d'obtenir une vitesse de chiffrement plus élevée. Mais cette tentative échoua, sans doute à cause de difficultés technologiques que l'on n'arrivait pas à maîtriser à l'époque et le projet fut abandonné. Un autre projet conduit par le lieutenant-colonel RAFFALLI, inspiré de la M209, fut aussi arrêté.

On s'orienta vers un autre système, étudié par la Marine et développé par la SAGEM : les TAREC, acronyme pour Translation Automatique Régénératrice Et Chiffrante. On savait qu'ils pouvaient assurer une grande sécurité s'ils étaient bien utilisés, et plusieurs pays de l'OTAN se mirent à en fabriquer. Les premiers TAREC ont commencé à entrer en service au milieu des années cinquante. Un avantage appréciable des TAREC était de pouvoir fonctionner, au choix de l'opérateur, en ligne ou hors ligne. Ces appareils (essentiellement ceux construits par la compagnie SAGEM) se répandirent alors dans les réseaux télégraphiques des administrations civiles et militaires.

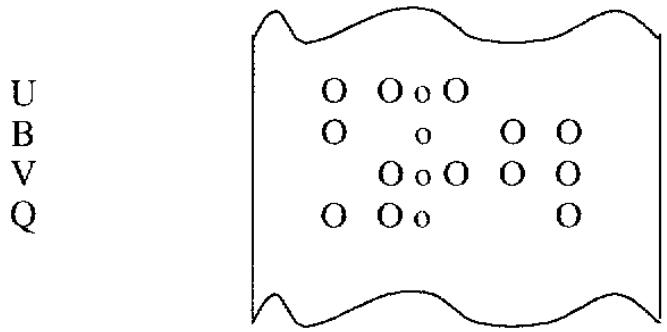
Ces machines reprenaient les principes du système Vernam (cf. l'annexe I, paragraphe 5). Elles utilisent des bandes (ou rubans) de papier perforées. Les perforations représentent des

bits : un trou code un bit valant 1, l'absence d'un trou représente un 0. Chaque caractère est représenté par un ensemble de cinq perforations (puisqu'en général un caractère est codé par cinq bits pouvant ainsi fournir trente-deux combinaisons) alignées suivant une perpendiculaire à l'axe de la bande. Ces bandes sont lues (ou perforées) caractère par caractère.

Un TAREC lit simultanément deux bandes : une bande dite « clé », préparée à l'avance, et, à l'émission, la bande contenant le message télégraphique à chiffrer. Les deux caractères ainsi lus sont combinés pour produire un caractère du crypto qui est perforé sur la bande « crypto » dans les cas d'un chiffrement hors ligne ou envoyé directement en ligne dans le cas d'un chiffrement en ligne. À la réception, le caractère reçu est le crypto ; combiné avec le caractère lu sur la bande clé, il fournit le clair correspondant qui est perforé sur la bande claire.

Voici comment se présente une bande perforée :

Caractères codés *Portion de ruban avec ses perforations*



En face des caractères on voit les perforations alignées qui codent chaque caractère. La troisième perforation (plus petite que les autres) ne code aucune information mais sert à entraîner le ruban par l'intermédiaire d'une roue dentée.

La bande « clé » devait être aléatoire et ne pouvait être utilisée qu'une fois pour garantir la sécurité voulue : c'est pourquoi on les appelait : *« bandes-clés une fois »*, c'est-à-dire clés à usage unique (*one time pad* en jargon anglo-américain ; aujourd'hui, les Canadiens francophones proposent de les appeler des « masques jetables »).

Le système de calcul utilisé à l'émission était le même pour chacun des cinq bits constituant les caractères (code à cinq moments). Il correspond à l'addition modulo 2 (ou addition sans retenue), conformément à la table suivante :

CLAIR	CLÉ	CRYPTO
0	0	0
0	1	1
1	0	1
1	1	0

On vérifie facilement qu'à la réception le même calcul entre le crypto et la clé redonne le clair, puisque cette table reste inchangée quand on permute la colonne du clair avec celle du crypto (autrement dit, cette opération est sa propre inverse).

Ces machines ne sont pas à proprement parler des machines à chiffrer, mais de simples additionneurs (modulo 2) munis de dispositifs de lecture et de perforation de bandes. Cependant ces systèmes sont théoriquement indécryptables à condition, d'une part, que l'aléa des bandes-clés soit de grande qualité et, d'autre part, que chaque bande-clé ne soit utilisée rigoureusement qu'une seule fois [5]. Si la première condition est relativement aisée à satisfaire par l'utilisation d'un ensemble de tests

[5] Si ces bandes sont utilisées plus d'une fois, c'est toute la sécurité du système qui est compromise. Cette contrainte est cependant difficile à respecter, souvent à cause d'incidents se produisant lors de la préparation ou de la transmission des messages, mais aussi d'erreurs des opérateurs. L'anecdote suivante est révélatrice de ce genre de difficultés.

En 1968, André MULLER décida de doubler le prix des bandes aléatoires qu'il fabriquait pour les différents organismes gouvernementaux. Il les vendait, jusqu'alors, à un prix dérisoire, très nettement en dessous de leur prix de revient. Cependant, un général, responsable des transmissions d'une des armées, refusa de doubler le budget correspondant. Il semble bien qu'il soupçonnait le STCCh d'avoir « inventé » la règle d'utilisation unique des bandes pour pouvoir en vendre plus ! Il ordonna à son chef du bureau « Chiffre » de commander la moitié des bandes dont il avait besoin, en lui donnant la consigne d'utiliser les bandes deux fois. Ce dernier expliqua, en vain, qu'une telle procédure était très dangereuse. Et il fallut l'intervention des plus hautes autorités du Chiffre pour faire revenir le général sur sa décision.

adéquats, en revanche la seconde qui est de nature organisationnelle est très difficile à appliquer et à vérifier. Elles constituent des exemples de machines à secret parfait (cf. le paragraphe 6 de l'annexe I) [6].

Cela ne signifie pas pour autant que ces machines basées sur des clés à usage unique soient inattaquables ! Bien au contraire, une mauvaise utilisation des clés peut anéantir toute leur sécurité [7]. De plus, les lecteurs-perforateurs de rubans, par les forts appels de courant qu'exige leur fonctionnement, présentent un rayonnement électromagnétique élevé qui peut compromettre gravement la confidentialité des informations traitées (voir le paragraphe II.4 de la deuxième partie).

Ces TAREC permettaient d'accélérer les opérations de chiffrement, mais la production des *« bandes-clés une fois »* et leur mise en place auprès des ateliers de chiffrement exige une logistique très lourde. Par ailleurs l'inconvénient du TAREC apparaît évident quand on constate qu'il interdit de travailler en réseau sous peine de voir la sécurité du chiffrement s'effondrer, sauf pour les réseaux en étoile, organisés autour d'un centre émetteur-récepteur travaillant avec les autres destinataires qui ne correspondent pas entre eux. La structure des réseaux des ministères de l'Intérieur ou des Affaires étrangères est typiquement en étoile (les ambassadeurs comme les préfets ne correspondent pas entre eux).

---

[6] Les TAREC ne peuvent pas être considérés comme des automates finis, car un opérateur les alimente en bandes-clés autant que de besoin, ce qui correspond à des automates potentiellement infinis (c'est-à-dire, des automates dont la mémoire, que constituent dans ces machines les bandes-clés, n'est pas bornée).

[7] Voir par exemple l'article de Louis RIBADEAU DUMAS, « Le projet Venona », *Bulletin de l'ARCSI*, n° 25, pp. 77-81. Ce projet Venona est une claire illustration de l'écart existant entre la sécurité théorique (ici, le secret parfait), prouvée mathématiquement, et la sécurité pratique correspondant aux conditions réelles d'utilisation. En effet, il est impossible de démontrer que les hypothèses de la preuve mathématique, qui sont de nature abstraite, sont en complète adéquation avec la mise en œuvre réelle du système de chiffrement, qui, elle, est de nature concrète. On ne peut que se contenter de vérifier expérimentalement que cette adéquation n'est pas ouvertement contredite par les faits.

Il faut noter que la distribution des bandes-clés, assurée par les organismes de gestion du Chiffre des départements ministériels, exige un canal sûr dont la capacité de transmission soit au moins égale à celle du canal normal de communication, lequel, par hypothèse, n'est pas sûr (puisque les clés doivent être aussi longues que les clairs). Le seul paramètre qui distingue ce canal sûr du canal ordinaire non sûr est le temps : on choisit le moment de transporter les bandes et on se donne le délai nécessaire correspondant au moyen de transport adopté. C'est ce degré de liberté, offert par le paramètre temps, qui permet de sécuriser ce canal, contrairement au canal de communication ordinaire [8].

En plus de ces matériels, subsistent normalement les moyens classiques manuels : essentiellement des codes et dictionnaires surchiffrés (souvent par carnets de clés ou par clés-blocs) qui perdureront jusqu'à la mise en service de moyens électroniques modernes. Au niveau tactique, outre des moyens de camouflage comme le Slidex, des machines à main mécaniques comme la CD57, compatible avec la CX52, constituent un notable progrès.

En revanche, aux niveaux supérieurs, la nécessité, d'une part, d'accélérer les opérations de chiffrement toujours trop lentes et l'existence, d'autre part, sur le marché de téléimprimeurs chiffrants, permettant de réaliser simultanément les opérations de chiffrement et de transmission (téléimprimeurs chiffrants Olivetti ou Siemens, dont le T-52 fut facilement décrypté par les Suédois, translations chiffrantes Lorenz, beaucoup plus solides ou les T-52 et T-55 d'HAGELIN), commandaient de s'orienter vers le chiffrement télégraphique automatique.

I.6. – LA SITUATION DÉFAVORABLE DU CHIFFRE FRANÇAIS À CETTE ÉPOQUE.

Il faut reconnaître que, dès cette époque, toutes ces machines (hormis les TAREC et la KL-7) sont d'une conception ancienne et, à part la CX52, présentaient une sécurité cryptologique toute

[8] L'anecdote (de Moscou) de l'annexe III montre cependant les limites d'une telle sécurisation.

relative. Par exemple la M209, malgré sa grande période, ne pouvait assurer le secret que pour quelques heures et son utilisation était limitée aux communications tactiques de bas niveau de confidentialité. Comme il n'existait pas de crédits pour financer des études, on se contentait de rechercher sur le marché les matériels qu'offraient les industriels. Ceux-ci proposaient en général des modèles ayant des possibilités de modifications afin de les personnaliser en fonction du client. L'EMA examinait ces possibilités et demandait au constructeur d'apporter aux machines achetées les modifications choisies.

En fait, il est triste de constater que la conception de ces machines, c'est-à-dire les travaux qui relevaient de la « défense », n'avait pas bénéficié des progrès techniques et scientifiques de l'époque et notamment de ceux réalisés au cours de la Seconde Guerre mondiale, alors que la cryptanalyse et, plus généralement, toutes les techniques et procédés relevant de « l'attaque », s'étaient considérablement perfectionnés, tant dans leurs méthodes que dans leurs outils.

En France, tout en sachant qu'il convenait de moderniser ces moyens, on semblait cependant s'en accommoder, car on ne soupçonnait pas ces énormes progrès. Les extraordinaires décryptements réalisés en Angleterre, à Bletchley Park lors du conflit de 39-45, restèrent longtemps secrets et ignorés des hauts responsables civils et militaires français. En particulier, les décryptements de la machine allemande Enigma, qui ont entraîné la construction de ces machines spéciales baptisées « les Bombes », et où s'illustra le grand mathématicien et logicien britannique Alan TURING, ne furent révélés qu'à partir de 1973.

Une autre avancée technologique considérable avait été réalisée par les Américains avec le système de cryptophonie digitale SIGSALY. Il était basé sur le vocodeur mis au point, dès 1939, par les *Bell Telephone Laboratories*. Ce vocodeur codait la parole en représentant son spectre sur douze canaux. Les échantillons de parole duraient vingt millisecondes et pouvaient avoir six niveaux d'intensité, ce qui représentait un débit équivalent de 1 800 bits/seconde. C'était la première réalisation de

modulation par impulsion (ou PCM : *Pulse Code Modulation*). Le chiffrement se faisait par une addition modulo 6 avec une clé à usage unique *(one time pad)* qui était obtenue à partir du bruit thermique d'un tube à vapeur de mercure. Cette clé était enregistrée sur un disque de vinyle. La capacité de ce disque permettait de chiffrer des conversations dont la durée ne pouvait excéder douze minutes. Comme les conversations téléphoniques duraient plus de douze minutes, un système de synchronisation très élaboré était nécessaire pour enchaîner le chiffrement entre deux lecteurs de disques consécutifs. L'équipement correspondant pesait 55 tonnes. Ce système, qui fut mis en service en juillet 1943, fut tenu secret jusqu'en 1976 !

L'arrivée des ordinateurs ne pouvait qu'aggraver la situation. Ainsi, on considère aujourd'hui, mais on l'ignorait dans les années cinquante, que le premier ordinateur électronique (programmable) fut la machine Colossus, construite à des fins cryptologiques par les Britanniques en 1943 (de mars à décembre). Elle fut utilisée pour décrypter les machines Lorenz (Zusatz 40 et 42) qui chiffraient le trafic des téléimprimeurs. Ces machines étaient utilisées par le haut commandement allemand pour communiquer avec les Armées. En août 1941, par suite d'une erreur de manipulation (ré-émission en ligne du même message chiffré avec la même clé, mais avec un décalage de quelques lettres dans le texte), la structure cryptographique des machines Lorenz fut révélée aux Alliés. Ceux-ci montèrent une section spéciale à Bletchley Park pour attaquer la machine. Les travaux montrèrent qu'il était possible de casser ce chiffre et des méthodes manuelles laborieuses furent mises au point : il fallait quatre à six semaines pour réaliser un décryptement ! Mais avec une machine Colossus, qui contenait 1 500 tubes électroniques et pesait plus d'une tonne, un décryptement ne prenait que quelques heures (une deuxième version de Colossus contenait 3 500 tubes).

Les premiers ordinateurs de la fin des années cinquante étaient incomparablement plus puissants que Colossus, tant en ce qui concerne la vitesse de calcul que la capacité de la mémoire. Ils étaient déjà beaucoup plus facilement programmables. Puis, en 1960, sont mises sur le marché les premières unités centrales à transistors (IBM 7090 ou le Gamma 60 de

Bull) ainsi que les mémoires à tores de ferrite qui allaient révolutionner l'informatique. La NSA *(National Security Agency)* américaine s'équipe en 1962 du calculateur le plus puissant du monde du moment : le « Stretch » (dont le nom commercial fut 7030) de la compagnie IBM. Ce calculateur pilotait un système de stockage des informations sur bandes magnétiques de 88 milliards de caractères sur 160 bandes (le système « Tractor »). C'est du Stretch que fut dérivé et mis sur le marché à partir de 1964, le célèbre System/360, première unité centrale à base de circuits intégrés. Enfin sont mis au point de nouveaux langages de programmation (Fortran, Algol, Lisp, APL, Simula, Cobol, Snobol, CPL...) et de nouveaux systèmes d'exploitation (permettant la multiprogrammation, le temps partagé...) qui, en créant l'industrie du logiciel, ouvrent de nouvelles perspectives en matière d'algorithmique : les méthodes de cryptanalyse les plus complexes et les plus subtiles pouvaient enfin être automatisées et appliquées à des masses de données considérables et ce, dans des temps extrêmement courts.

On sait que, durant la Deuxième Guerre mondiale et malgré les vicissitudes de la situation de la France, les services français réalisèrent, avec les moyens du bord, de nombreux décryptements et, en outre, contribuèrent grandement, par les renseignements fournis, aux décryptements britanniques de l'Enigma [9]. Mais ils furent tenus à l'écart des travaux qui se faisaient à Bletchley Park, dont ils ignorèrent tout : les quelques Français ayant collaboré à Bletchley Park se turent aussi jusqu'en 1973. Les services français n'eurent donc pas l'occasion de se familiariser avec ces nouvelles techniques ni même d'en présumer la valeur. Cette situation était d'autant plus défavorable pour le Chiffre français que les militaires considéraient que le Chiffre ne servait qu'à ralentir les transmissions (on avait encore le souvenir de la campagne de mai-juin 1940) !

---

[9] Il semble que, sur une initiative du général COLSON, chef d'état-major des Armées, des travaux analogues à ceux de Bletchley Park aient eu lieu en France, dans les premières années de la guerre, au sein de la compagnie des machines Bull pour décrypter l'Enigma (cf. l'article paru dans le numéro 23 [1995-1996], p. 41 du *Bulletin de l'ARCSI*).

DEUXIÈME PARTIE

LA CONCEPTION DE MYOSOTIS LE CONCOURS NATIONAL ET LE CONCOURS OTAN

II.1. – LES PRÉMICES DU CONCOURS INTERNE FRANÇAIS.

L'intervention franco-britannique de Suez, en 1956, avait mis en évidence l'inadéquation de nos moyens de chiffrement, tant nationaux que OTAN. En effet, nos alliés britanniques nous firent savoir qu'il ne fallait plus utiliser la B211 : celle-ci devait être considérée comme périmée ; en outre les délais de chiffrement et de déchiffrement étaient apparus largement excessifs. Par ailleurs, il semble bien que les messages alliés étaient interceptés sur le sol égyptien, puis transmis à Moscou où ils étaient décryptés.

Cela fut un choc considérable pour les militaires. On décida de retirer la B211 des services et d'utiliser à la place la machine américaine KL-7. Celle-ci est alors fournie aux Armées, dans le cadre de l'OTAN.

Sous l'impulsion d'André MULLER, les autorités gouvernementales décidèrent de rénover nos moyens de chiffrement. Un plan de modernisation des équipements fut lancé et approuvé en 1957 par la CIC. Des crédits furent débloqués aux Armées. On acheta d'abord la licence de fabrication de la CX52. Puis on s'orienta vers la conception d'une nouvelle machine et la décision de lancer l'étude d'une machine à chiffrer télégraphique fut prise.

Les trois armées voulaient chacune en faire une et une guerre des « boutons cryptologiques » commença. La Marine entrepris d'étudier la machine « Ulysse » à laquelle allait collaborer la SEA. Mais la Marine devait se retirer assez rapidement. L'armée de l'Air, avec principalement le colonel ANTOINE, se lança dans la conception d'une machine à partir de la KL-7 ; celle-ci est devenue « Violette » et a été étudiée par la SAGEM.

Mais c'est Marius GAUBERT, représentant la SEFT à la sous-commission « Cryptologie » qui, vers la fin de l'année 1958 ou le tout début de 1959, soumet une idée vraiment originale. Celle-ci consiste à effectuer le calcul du crypto en tirant des alphabets aléatoires [10]. Cette idée est discutée par la sous-commission qui, naturellement, la trouve très intéressante. Mais si, sur le plan théorique cette idée est séduisante, encore faut-il démontrer, d'une part, qu'un tel organe de calcul, capable de fonctionner avec la vitesse voulue, est réalisable, d'autre part, que l'on sait faire un générateur d'aléa capable de fournir les suites de lettres nécessaires pour constituer les alphabets aléatoires. Ce générateur d'aléa devait offrir un haut niveau de résistance aux attaques cryptographiques connues tout en respectant les exigences du trafic envisagé pour cette machine ! En l'occurrence, il s'agissait d'un générateur pseudo-aléatoire, puisque le destinataire devait pouvoir fabriquer les mêmes alphabets aléatoires pour déchiffrer les messages.

C'est le colonel RIBADEAU DUMAS qui s'attaque, au début de 1959, à la première condition de faisabilité : il s'agit de déterminer le nombre de tirages minimum permettant d'obtenir, avec une bonne probabilité, les alphabets voulus, sachant qu'il fallait envisager des alphabets à 26, 27, 31 ou 32 lettres. RIBADEAU DUMAS aboutit à des formules très compliquées à calculer numériquement, surtout à l'époque où l'on ne disposait pratiquement pas d'ordinateurs et où les machines à calculer étaient très rudimentaires. La principale difficulté était de devoir effectuer énormément de calculs avec une très grande précision, car il fallait soustraire de très grands nombres dont les valeurs étaient très voisines. RIBADEAU DUMAS réussit à définir des conditions d'approximation et les formules approchées correspondantes. Il parvint à effectuer une première série de calculs permettant de déterminer les longueurs de tirages nécessaires. Ainsi dans le cas d'un alphabet de 31 lettres (le

[10] Il semblerait que l'idée de tirer un alphabet aléatoire pour traiter chaque lettre ait germé au CECS parmi les stagiaires, mais on ne savait pas comment la réaliser. L'idée aurait été exposée à Marius GAUBERT qui a su la mettre en pratique par le mécanisme du chiffrement à la volée !

32e caractère n'étant pas utilisé en télégraphie), il trouve qu'il faut 127 tirages pour obtenir un alphabet complet avec une probabilité d'environ 90 %.

Une première condition que doit satisfaire la machine est ainsi établie. Si le résultat obtenu par RIBADEAU DUMAS ne paraît pas incompatible avec la technologie de l'époque, on est encore loin de la définition d'une machine à chiffrer et de la preuve de sa faisabilité !

Partant à Oran, RIBADEAU DUMAS arrête là ses travaux. À son retour en 1962, la machine Myosotis est déjà bien avancée. André MULLER lui demandera tout de même de revenir à la sous-commission « Cryptologie », où il participera à la suite des travaux et surtout à la décision finale.

II.2. – LES PREMIERS CONTACTS DE LA CSF AVEC LE CHIFFRE.

Le commercial de la CSF, chargé de l'armée de Terre, M. MOINEAU, était camarade de promotion de l'École Polytechnique du directeur de la SEFT, à savoir l'ingénieur général REVIRIEUX. En 1959, il apprend par ce dernier que la SEFT voulait transistoriser le système mécanique permettant le brouillage des communications hertziennes selon le principe du découpage de bande dont on a parlé plus haut. En fait, il s'agissait d'un matériel de cryptophonie à quatre bandes, le DT414, développé par l'armée de Terre. Celui-ci était piloté par un système mécanique de la société CAMECA.

M. MOINEAU avertit Xavier AMEIL. Celui-ci organise la première relation technique (mais aussi gastronomique !) entre l'ingénieur en chef GAUBERT, chargé du projet au sein de la SEFT, et le spécialiste à Puteaux des études de transistorisation, Jean-Pierre VASSEUR. Le projet prend corps. Ce travail est réalisé dans le cadre d'un marché passé au centre de Levallois et un prototype est réalisé. C'est en fait, pour Jean-Pierre VASSEUR, l'occasion de commencer à réfléchir à ce que pourrait être une machine à chiffrer électronique.

Il a alors la possibilité de développer ses idées quand, pendant l'été 1960, la SEFT propose à RPC de mettre au point une maquette d'un équipement de chiffrement de fac-similé, ceci dans le cadre d'un contrat de l'armée de Terre avec les États-Unis. RPC répond positivement et Jean-Pierre VASSEUR en est chargé. Une équipe est constituée et les principaux responsables de la réalisation sont Jacques RIETHMÜLLER, spécialiste de l'électronique, et Marc DUMAIRE qui est embauché à RPC à cette occasion, en septembre 1960. Il apporte, en particulier, sa compétence dans la conception des circuits logiques. Marc DUMAIRE venait de la SEA, la compagnie d'informatique créée par François-Henri RAYMOND. Cette société était connue pour les ordinateurs originaux qu'elle fabriquait, dont les célèbres CAB 500 et 1 500. Comme nous l'avons dit plus haut, la SEA était impliquée aussi dans le chiffre avec la machine Ulysse, mais il faut préciser que Marc DUMAIRE n'y avait pas pris part.

Dans ce projet de chiffrement de fac-similé, si la synchronisation de la liaison fax était un des points délicats à résoudre (il faut en particulier définir avec précision le point de départ du message) les algorithmes nécessaires au chiffrement retiennent l'attention de Jean-Pierre VASSEUR qui voyait là une étude particulièrement fertile pour la suite. Il a d'ailleurs l'occasion de constater qu'en dépit d'une algorithmique très élaborée, mise en œuvre par une électronique complexe, on pouvait obtenir des fax chiffrés qui laissaient deviner certains éléments du clair ! En effet, les images sont extrêmement redondantes et l'information qu'elles contiennent est très difficile à masquer. C'est par une analyse statistique poussée que l'on a pu mettre en évidence l'origine du défaut et apporter la correction correspondante.

II.3. – LE DÉBUT DE L'AFFAIRE MYOSOTIS.

C'est au cours de ces premiers travaux qu'une grande amitié s'établit entre Marius GAUBERT et Jean-Pierre VASSEUR. Ils en viennent rapidement à parler des machines mécaniques de chiffrement existant alors (ou de nouvelles à concevoir ?) et

de leur éventuelle transistorisation. Qui en a eu le premier l'idée : GAUBERT, VASSEUR... ou les deux ? Et surtout ils discutent de l'idée du tirage des alphabets aléatoires. Beaucoup de problèmes restaient à régler, en particulier celui de compléter l'alphabet quand la suite des tirages n'a pas fourni toutes les lettres voulues, sans détruire le caractère aléatoire du début de l'alphabet déjà obtenu.

La force de l'idée de GAUBERT, c'était de pouvoir effectuer le chiffrement à la volée, sans avoir à mémoriser l'alphabet chiffrant. C'est pourquoi Marius GAUBERT, très au fait des questions de cryptographie, dépose un brevet le 1er août 1960 (brevet n° 834596). L'évolution de l'électronique que l'on pressentait déjà permettait d'espérer que ce principe pouvait être rendu compatible avec les exigences de vitesse des transmissions télégraphiques (50 et 75 bauds), compte tenu des composants électroniques industriellement disponibles. Jean-Pierre VASSEUR a immédiatement vu un grand intérêt dans ce brevet, surtout si on pouvait le coupler avec le système de génération de clé auquel il réfléchissait. L'idée de construire un prototype d'évaluation prend corps.

Par ailleurs, l'OTAN lançait à ce moment un concours pour réaliser un prototype de machine cryptographique pour la télégraphie et dont l'échéance de présentation des matériels était février 1963 (nous revenons sur ce concours aux paragraphes suivants).

Quel qu'en soit l'initiateur, le fait important est que le laboratoire de recherches physico-chimiques de la CSF a pris la décision d'étudier et de réaliser sur fonds propres un tel prototype, décision qui n'avait pas la totale bénédiction du directeur technique du laboratoire, Claude DUGAS, ce dernier pensant, à juste titre, qu'un laboratoire de composants n'est pas destiné à étudier et réaliser des prototypes de matériels.

L'équipe de VASSEUR travaille donc d'arrache-pied car le délai de présentation à l'OTAN est très court. Deux maquettes de démonstration en valise sont réalisées pour une présentation aux Armées, dans le bureau de M. André DANZIN, directeur du groupement « Matériaux et Composants ».

Ces maquettes mettent déjà en évidence les points forts de Myosotis. Une des caractéristiques importantes de Myosotis était son système de mise à la clé du jour : VASSEUR en inventant les permutateurs enfichables réalisait un progrès considérable par rapport aux systèmes utilisant des câbles. Ces permutateurs se sont révélés très fiables et faciles à utiliser : la mise à la clé du jour était beaucoup plus facile et plus sûre qu'avec des câbles enfichables. Ils permettaient de définir un très grand nombre de clés. On comparera, par exemple, le nombre de clés de Myosotis (annexe II) et celui de la KW-7 (paragraphe II.5). Cependant ils furent le prétexte de nombreuses critiques de la part des Anglo-Saxons lors du concours OTAN (cf. le paragraphe II-6).

Autour de l'idée des permutateurs, VASSEUR applique plusieurs principes fondamentaux, souvent inspirés de la théorie de SHANNON :

- introduire des circuits non linéaires ;
- obtenir l'équiprobabilité des variables binaires internes ;
- casser les corrélations entre ces variables en les rendant statistiquement inexploitables ;
- créer de la confusion et de la diffusion entre les informations ;
- introduire le maximum d'ambiguïté entre les informations internes de la machine et le crypto.

La fréquence d'horloge choisie est aussi élevée que possible pour pouvoir atteindre les plus hauts débits de cette époque (2 400 bits/s). Mais ceci pose des problèmes complexes de consommation et d'échauffement, d'autant plus difficiles à résoudre que les contraintes d'ambiance imposées par les Armées sont sévères.

Enfin, VASSEUR pense à tous les mécanismes auxiliaires nécessaires pour faciliter le travail des opérateurs et diminuer les risques d'erreur : mise en opération, synchronisation, détection des pannes, alarmes, maintenance.

Dès que les premiers résultats sont prometteurs, Jean-Pierre VASSEUR et Xavier AMEIL, accompagnés de Jean-Charles

DEVIN, PDG de LCC et chargé en outre des problèmes internationaux pour la division « Composants », demandent audience au PDG de la CSF, Maurice PONTE. Il faut, en effet, le mettre au courant de cette affaire et qu'il veuille bien approuver cette décision. L'argument majeur présenté est que le délai de réalisation d'un prototype de machine est si court qu'il est pratiquement impossible de le faire réaliser par une équipe de matériel, peu habituée aux possibilités des éléments semi-conducteurs et surtout ne connaissant pas intimement l'ingénieur en chef GAUBERT dont la collaboration était indispensable. À l'issue de l'entretien Maurice PONTE donne son accord avec un crédit exceptionnel d'études internes.

Il est décidé que Jean-Pierre VASSEUR rapporterait directement à Maurice PONTE pour la suite des travaux.

De son côté, Maurice PONTE se charge de calmer les dirigeants de la division « Matériels ». En effet, ceux-ci voyaient d'un mauvais œil le fait de ne pas être dans le coup dès le départ dans le futur marché de la cryptographie qui était seule envisagée, au premier abord. Mais, en fait, les matériels prototypes ont tout de même été réalisés avec les moyens de Levallois.

Il faut dire que Maurice PONTE avait tout de suite compris l'intérêt du secret pour une compagnie dont une des activités principales était la communication par radio. En outre, il s'intéressait beaucoup à la technique et visitait le laboratoire environ deux fois par mois. Jean-Pierre VASSEUR allait lui rendre compte assez souvent dans son bureau. Son appui personnel a été déterminant dans le succès de Myosotis. Maurice PONTE avait créé les crédits de recherche « du Président », dont il était seul à disposer. On en obtenait assez facilement, mais Maurice PONTE devenait sans pitié si l'on avait abusé de sa confiance. C'est sur ces crédits que le projet Myosotis a été lancé.

C'est vraisemblablement à cause du délai très court de présentation des matériels que la direction de la SEFT n'a accordé à la CSF aucun marché d'études en dehors de celui du Fax. La lenteur d'obtention du marché aurait eu pour conséquence que celui-ci n'aurait été approuvé qu'après que le prototype eût été achevé. Une autre raison compréhensible est que, voyant la CSF

tellement engagée financièrement dans cette affaire, la SEFT faisait une économie et n'entrait pas dans cette étrange situation de financer une unité de composants pour réaliser un matériel.

II.4. – LE LANCEMENT DU CONCOURS OTAN.

Peu de temps après l'expédition de Suez, l'OTAN décide aussi de moderniser les moyens cryptologiques de l'Alliance. Le comité militaire lance alors un appel à candidature pour une machine à chiffrer télégraphique électronique, sur la base de spécifications militaires mises au point par l'ACSA *(Allied Communications Security Agency).* Entre autres spécifications, il était précisé que la machine devait être sans bande, ni rotor *(tapeless and rotorless),* donc pas de systèmes utilisant des « bandes-clés une fois », ni de machines électromécaniques dérivées de l'Enigma, comme la KL-7.

Elle devait avoir les deux modes de fonctionnement : en ligne ou hors ligne. En outre, l'ensemble de la station de chiffrement devait répondre à des contraintes très sévères concernant le rayonnement et la conduction électromagnétique des circuits véhiculant des informations claires traitées par la machine (contrainte TEMPEST) [11]. Le problème du rayonnement avait été posé au début des années cinquante par une machine à bande aléatoire qui utilisait des relais dont la commutation du contacteur provoquait des étincelles accompagnées d'un très fort rayonnement dans lequel on pouvait retrouver des informations claires. Il semble que les Américains avaient eu connaissance que ce phénomène avait été exploité à Moscou au détriment de leur ambassade. Le cahier des charges indiquait simplement « aucun rayonnement détectable », sans préciser les conditions de mesure !

Il faut ajouter que le cahier des charges original, rédigé en anglais, avait été mal traduit en français et a été, sur plusieurs points, mal compris, et notamment sur l'aspect opérationnel. Heureusement, le commandant RABAUD, fort de son expérience de l'exploitation, a su définir les modifications à apporter au

[11] TEMPEST signifie : Transcient ElectroMagnetic Pulse Emanation Standard.

bloc de commande de Myosotis pour être conforme aux exigences OTAN.

La technologie électronique en circuits discrets de l'époque et les transistors, qui venaient d'être inventés (1948), allaient permettre une souplesse et une complexité de conception cryptologique jamais atteinte par la technologie électromécanique antérieure. En outre, une rapidité de traitement supérieure aux vitesses télégraphiques usuelles était envisageable : le sempiternel reproche de lenteur fait au Chiffre allait enfin tomber ! Il est vrai que l'électronique des années cinquante utilisait presque exclusivement des lampes (tubes à vide : diodes triodes, pentodes...). Mais le nombre de circuits nécessaires rendait la réalisation d'une machine à chiffrer à lampes totalement irréaliste. Il était temps de songer à recourir à l'électronique des composants solides, celle des semi-conducteurs, pour réaliser de nouvelles machines.

Il s'agissait non seulement d'améliorer les qualités cryptographiques de ces machines, mais aussi leurs conditions d'utilisation en automatisant plus de fonctions dans un volume plus faible et en les rendant plus maniables pour réduire les erreurs d'exploitation. En outre, l'électronique à semi-conducteur diminuait considérablement le poids, l'encombrement et la consommation, donc l'alimentation. Ceci allait dans le sens d'un élargissement du domaine d'emploi des machines, surtout pour les besoins tactiques, et permettait d'envisager des systèmes embarqués ou portables. Il fallait aussi satisfaire les nouvelles exigences des télécommunications, en particulier l'augmentation de la vitesse de transmission.

La Défense décide de répondre et de participer à ce qu'on appellera le « concours OTAN », puisque d'autres pays vont aussi présenter leurs matériels.

II.5. – LES MACHINES ÉTRANGÈRES CONCURRENTES DE MYOSOTIS.

Trois autres pays ont participé au concours OTAN : les USA, qui présentaient la machine KW-7 ; le Royaume-Uni, la machine ALVIS ; l'Allemagne, l'ELCROTEL.

Plus tard, la France eut quelques indications sur ces machines.

La KW-7 était entièrement transistorisée. Sa logique était plus simple que celle de Myosotis et l'aléa qu'elle produisait était certainement de moins bonne qualité en raison de la présence de corrélations temporelles assez évidentes. Mais surtout le calcul du crypto était beaucoup plus rudimentaire : c'était une simple addition modulo 2, bit à bit. Ce calcul était donc très sensible aux attaques basées sur les messages parallèles, bien qu'il utilisât un dispositif d'autoclave par caractère sur cinq bits.

Mais le principal avantage de la KW-7 était l'utilisation d'un registre « R » linéaire et à période maximale, dont la structure était définie par un polynôme primitif de degré 39. Ce registre comportait donc 39 pas et avait un avancement irrégulier. Il assurait une période minimale importante : $6{,}87.10^{11}$, environ. Cependant la période moyenne de la KW-7 ($5{,}5.10^{12}$, environ) était comparable à celle de Myosotis (3.10^{12}, voir le paragraphe 3.1 de l'annexe II).

Précisons que la théorie de ces registres à période maximale était très peu répandue à cette époque : les publications de D.A. HUFFMAN, qui établissaient un lien entre ces registres et les codes correcteurs d'erreurs, ne datent que de 1956. Et encore, ce sont les travaux postérieurs de BOSE et CHAUDHURI, publiés en 1960, qui ont attiré l'attention des concepteurs de circuits logiques séquentiels sur ces registres. En fait, BOSE et CHAUDHURI avaient été légèrement devancés par le Français A. HOCQUENGHEM, mais son travail, publié en 1959 dans la revue française *Chiffres*, était passé inaperçu.

La mise à la clé du jour de la KW-7 consistait à connecter trente entrées de portes logiques avec les trente et un premiers étages du registre R. En admettant que toutes ces combinaisons définissent autant de configurations distinctes, cela représente un nombre total de clés de :

$$K = 31\,! = 8{,}2.10^{33}.$$

La KW-7, qui pesait à peu près 40 kilogrammes pour un volume de 50 litres, a été construite selon deux variantes dont

les mises à la clé étaient différentes. Dans la première, on établissait les connexions manuellement avec des câbles que l'on enfichait dans des prises sur un tableau de branchement. Ce système, assez archaïque et rappelant étrangement la machine allemande Enigma, était très peu commode, d'une mise en œuvre assez pénible et sujette à l'erreur. La deuxième variante utilisait des cartes perforées inspirées des machines IBM. Ce système était plus commode mais nécessitait un matériel spécial de perforation pour préparer les cartes. Ces deux variantes n'étaient pas compatibles et ne pouvaient communiquer entre elles ! La Marine américaine adopta la variante à cartes perforées, tandis que l'armée de Terre adopta la machine à câbles. La KW-7 resta en fonction jusqu'en 1988.

L'exploitation et surtout la maintenance de la KW-7 étaient assez laborieuses, car la détection des pannes était très difficile. Cette machine exigeait un à deux mois de formation. Sa principale protection contre les indiscrétions était un capot dont le verrou se manœuvrait à l'aide d'une clé plate. Pour des raisons de sécurité, celle-ci était très difficile à reproduire car elle comportait trois rangées de dents (une rangée d'un côté et deux de l'autre) [12].

La machine ALVIS aussi utilisait un registre linéaire à période maximale. Mais le reste de la logique était relativement peu complexe et on peut s'interroger sur sa valeur cryptologique. La taille de la machine était impressionnante : c'était une baie d'environ deux mètres de haut et soixante centimètres de large, contenant six gros tiroirs d'électronique. La mise à la clé du jour de la machine consistait à configurer un tableau de branchements. Cette configuration était réalisée par deux cartes

[12] Signalons qu'en 1985, un officier du Chiffre de la Marine américaine, John WALKER, fut arrêté pour espionnage. Depuis 1967, celui-ci vendait régulièrement au KGB les clés (et quelquefois les manuels de maintenance) de tous les systèmes de chiffrement utilisés par la Marine américaine. Il fournissait donc, en particulier, celles de la KW-7 à cartes perforées. Comme l'URSS s'était par ailleurs procurée cette machine en d'autres occasions (au Vietnam et lors de la capture du Pueblo, en janvier 1968, par l'armée nord-coréenne), cela signifie que ce pays lisait tous les messages secrets américains qu'il pouvait intercepter depuis plus de dix-sept ans !

de circuits imprimés (d'environ 8 cm sur 12) que l'on introduisait dans des connecteurs. Ces cartes contenaient trente câbles soudés sur une rangée du bas ; ces câbles devaient être enfichés dans des prises situées sur ces cartes dans trois rangées au-dessus. Ces cartes pouvaient être préparées à l'avance mais elles étaient relativement fragiles et sujettes à de nombreuses pannes (coupures ou mauvais contacts des câbles).

Quant à la machine allemande, nous n'avons pas eu beaucoup d'informations sur elle. Il semble que sa logique présentait quelques similitudes avec celle de Myosotis. Sa mémoire était une matrice de tores de ferrite. Mais c'était une machine volumineuse et son bloc de commande était une fois et demi plus gros que le bloc de chiffrement. Comme sa fréquence de fonctionnement était relativement élevée pour l'époque : 500 kHz, on a pu, par la suite, en faire une version, appelée Elcrovox, adaptée à la cryptophonie grâce à un vocodeur fonctionnant à 2 400 bits/s (le docteur GOING du ZfCh était un spécialiste des vocodeurs).

II.6. – LA PRÉSENTATION DE MYOSOTIS AU CONCOURS OTAN.

C'est donc en 1961 que la CSF, en accord avec le SEFT et pour le compte de l'armée de Terre, se lance dans ce concours, en troisième position car il y avait déjà deux autres projets en lice : les machines Ulysse de la SEA et Violette de la SAGEM. Mais, finalement, seule Myosotis sera présentée au concours OTAN.

Ce nom de Violette a peut-être donné l'idée à Marius GAUBERT [13] de donner aussi un nom de fleur au prototype de la CSF : il propose Myosotis... Mais par ce choix, il voulait sans doute faire un double jeu de mots pour rappeler à la CSF que l'on n'oublie pas son brevet, mais aussi aux Armées

[13] En fait c'est MULLER qui aurait lancé l'idée, sans doute à la sous-commission « Cryptologie », d'adopter des noms de fleurs pour les divers projets de machines (mais que la Marine n'aurait pas suivie !).

qu'elles n'oublient pas Myosotis (myosotis se dit en anglais : *forget-me-not ;* ce qui se traduit mot à mot en français : ne m'oubliez pas !).

Le concours OTAN comportait trois phases : un examen au SHAPE à Rocquencourt, des essais opérationnels dans l'air, sur mer et sur terre, et enfin une évaluation cryptologique à Washington.

Le délai de février 1963 imposait une équipe solide et performante pour réaliser en moins de dix-huit mois les trois prototypes destinés à être testés dans les conditions opérationnelles par les différentes Armées. Il fallait donc un appui industriel que VASSEUR trouva auprès du centre de Levallois, centre que, par ailleurs, il connaissait bien pour y avoir fait ses débuts à la CSF.

Le service de Levallois met alors en place une équipe ayant déjà l'expérience du DT 414. Cette équipe, placée sous la responsabilité de la direction des études, est menée par un binôme d'ingénieurs : MM. SEIGNOL et SAMAIN. Ils surent allier organisation et savoir-faire technique avec le responsable du développement et le bureau d'étude pour réussir à sortir le matériel en moins d'un an. En fin d'année 1962, les minutes comptaient et ne laissaient guère de place aux festivités. SEIGNOL, qui venait d'avoir un fils, eut beaucoup de mal à trouver le temps pour aller le déclarer à l'état civil !

En février 1963, c'est la présentation au SHAPE. Le matériel en cours faisait l'objet de nombreux essais à RPC où l'approche de la date de présentation au SHAPE s'est traduite pour les équipes par quelques nuits passées dans le laboratoire de Puteaux : dans les dernières semaines des lits de camp avaient été installés dans le laboratoire et le travail se faisait en continu. La veille de la présentation à Rocquencourt, le matériel est tombé en panne et rien ne marchait. Vers minuit, les techniciens recommandèrent à VASSEUR d'aller se coucher, sans doute pour se débarrasser de lui car il n'avait plus à y intervenir, mais en lui disant : « Il vaut mieux que vous dormiez, vous devez être en forme demain matin pour faire la présentation. » Et la machine fut à l'heure au rendez-vous et en état de marche !

Le matériel, officiellement présenté par l'armée française, avait été transporté sous escorte militaire. Les clés, qui avaient été faites par RABAUD, furent scellées dans des enveloppes opaques aux rayons X.

Comme pour les autres concurrents, à Rocquencourt, il y eut une première série d'examens par les services américains. On se rendit compte à Rocquencourt que le concours était très partial. Par exemple, une panne se produisit, mais elle fut vite réparée par nos techniciens qui étaient sur place. Mais la délégation anglaise en a aussitôt profité pour demander l'élimination de Myosotis. Les Français durent faire appel ; la demande anglaise fut âprement discutée et finalement elle fut tout de même refusée : Myosotis restait en course !

Les Anglo-Saxons, qui préféraient les câbles aux permutateurs (sans doute parce qu'ils n'en avaient pas eu l'idée !), émirent à leur encontre des critiques injustifiées :

- ils les assimilaient à des rotors, alors que leur rôle était très différent (ils ne tournaient pas et associés aux codeurs et aux décodeurs, ils introduisaient une fonction non linéaire d'une très grande force cryptographique) ;
- ils soulignaient qu'ils pouvaient être capturés et donc pouvaient compromettre la sécurité de Myosotis, alors que celle-ci ne reposait nullement sur le secret des permutateurs !

En mars, le matériel est expédié pour procéder aux essais opérationnels : aéroportés, embarqués sur deux bateaux de la Marine américaine et sur une station terre à Malte. Les essais aéroportés furent organisés à partir de la base américaine d'Évreux, sous le contrôle du *Silk Purse Control Group,* qui constituait le PC volant de l'US Air Force en Europe. Côté français, le responsable était le commandant Christian FABRE de la base aérienne 134. Son interlocuteur principal était le major COOPER, qui lui servait en même temps d'interprète.

Les essais se sont étalés sur une période de deux mois. Les vols, qui se déroulaient sur un quadrimoteur du type DC7, duraient douze heures, mais seule une demi-heure était vraiment

opérationnelle. Ils consistaient à survoler la Champagne. La base d'Évreux était assez souvent sujette au brouillard : plusieurs atterrissages ont été plus qu'acrobatiques et une fois l'avion a dû être détourné sur la base américaine de Torrejón en Espagne ! Les essais concernaient Myosotis et la KW-7 qui était embarquée sur le même avion. Ils étaient réalisés par une équipe américaine composée de deux officiers supérieurs et d'un sous-officier. Ils opéraient dans une zone centrale de l'avion équipée de moyens de télécommunications, où ils communiquaient avec Malte, mais où les Français n'avaient pas le droit d'aller.

La principale difficulté de ces essais était la transmission des clés, car les Français, qui n'avaient pas eu le temps de s'y préparer, n'avaient pris aucune précaution contre d'éventuels problèmes de communication. Or la liaison s'est révélée très défectueuse et cela entraîna beaucoup d'erreurs de transmissions, donc des clés erronées, qui ont dû être retransmises plusieurs fois. En revanche, les Américains avaient mis en place des procédures de transmissions robustes avec des codes redondants très efficaces. On constata une fois encore la mauvaise fois des Anglo-Saxons, qui attribuèrent ce défaut à Myosotis, alors qu'elle n'y était pour rien !

Puis eut lieu la préparation de la mission à Washington auprès de l'Agence d'évaluation du comité militaire de l'Alliance (SECAN). C'est ce laboratoire qui doit procéder à l'évaluation cryptologique du matériel et proposer au comité militaire son approbation pour la protection des informations classifiées de l'OTAN [14].

Pour cette dernière épreuve, on s'aperçoit assez vite que le concours est « pipé » car ce laboratoire a mis aussi au point un prototype pour une firme américaine. Il n'y avait donc aucune chance de gagner. Mais pour se consoler, on peut dire que, grâce à ce concours, Myosotis, la machine de la CSF, s'est

[14] Selon les règles de l'OTAN, pour chiffrer du secret OTAN avec un procédé national, celui-ci doit avoir obtenu l'aval du comité militaire, donc du SECAN.

trouvée dans une bonne position pour devenir la machine de chiffrement commune à toutes les administrations françaises.

À Washington, l'équipe est installée dans un bâtiment de l'ambassade de France. Son mentor est le capitaine de vaisseau Henri LAVOLLAY, membre de l'équipe de l'attaché militaire près l'ambassade de France. Il fera tout son possible pour faciliter la mission confiée à MM. DUMAIRE et CORRÉARD. Le matériel est présenté aux agents du SECAN qui se familiarisent avec son fonctionnement. Toute la documentation, rédigée en anglais, leur est communiquée ; cela dure une quinzaine de jours, au terme desquels, le matériel est transféré au SECAN qui prend en main tous les équipements sans que l'équipe française puisse intervenir. En particulier, l'étude statistique, dont nous parlons au paragraphe II.8, leur fut aussi intégralement transmise. Mais le SECAN ne fit aucun commentaire à ce sujet, comme d'ailleurs pour les autres éléments de son évaluation.

Parmi les contrôles effectués, outre ceux relatifs à la qualité cryptographique de la machine, les Américains ont demandé aux Français de calculer (essentiellement à la main) quelques cryptos de Myosotis, sans leur laisser la possibilité de l'utiliser. Le but de cette demande était de vérifier que son fonctionnement réel était bien conforme à la documentation fournie. C'est CORRÉARD qui opère ce chiffrement manuel. C'est un véritable exploit que réalise là CORRÉARD, car pour effectuer correctement ce calcul, qui représentait un nombre gigantesque d'opérations logiques, il fallait connaître les plus petits détails de la machine, et bien sûr ne jamais se tromper alors que rien n'est plus facile que de confondre les 0 et les 1 !

CORRÉARD met deux semaines pour effectuer ces calculs et finalement, les Américains vérifient que le résultat fourni est bien identique à ce que trouve Myosotis ! M. CORRÉARD restera une quinzaine de jours supplémentaires pour pallier un éventuel problème.

Finalement, l'OTAN choisit la machine anglaise ALVIS, laquelle était la plus chère et sans doute la moins bonne !

Mais, environ six mois plus tard, le STCCh informera la CSF du résultat de l'évaluation par SECAN : Myosotis obtient

l'approbation du comité militaire pour la protection des informations de toutes classifications OTAN. La machine Myosotis est donc approuvée OTAN. C'est un beau succès [15] !

Pour la petite histoire, André MULLER apprendra plus tard que les Américains avaient trouvé que Myosotis était en fait la meilleure machine ; mais d'autres considérations avaient prévalu !

II.7. – LES CONCURRENTS FRANÇAIS DE MYOSOTIS.

Pendant ce temps que faisaient les deux autres services de télécommunications militaires qui étaient au courant du concours OTAN ?

Le STTA avait supporté financièrement la SAGEM qui étudiait un prototype de machine qu'elle avait baptisée Violette. Cette machine était caractérisée par sa compatibilité avec la KL-7 et ses permutateurs Sillet. Ces permutateurs permettaient de découper les alphabets en deux parties et, par composition, de créer des alphabets « aléatoires ». En fait Violette avait deux modes de fonctionnement. L'un était une émulation de la KL-7, l'autre était plus compliqué. La théorie était inspirée des idées de M. SUCHARD qui enseignait les probabilités et l'informatique à l'université de Paris. Mais la logique de Violette étant proche de l'esprit « rotor », elle était mal placée pour le concours OTAN qui précisait « rotorless ». En outre, elle utilisait des thyratrons à cathode froide, qui se sont révélés être un sérieux handicap : manque de fiabilité et de discrétion (problème TEMPEST), poids et volume très importants, etc.

On peut se demander pourquoi, antérieurement, le STTA, qui faisait travailler la CSF sur des sujets touchant de près à la sécurité des télécommunications, ne lui a pas proposé de concourir au projet OTAN ? Une explication découle peut-être

[15] Mais il faut avouer que ce fut une victoire à la Pyrrhus : la France devait sortir de l'organisation militaire du traité de l'Atlantique Nord en mars 1966, de sorte que la CSF n'eut guère l'occasion de fournir des matériels de chiffrement aux armées de l'OTAN. Et les services américains étaient en possession de tous les détails de Myosotis !

de la volonté du directeur du STTA, l'ingénieur général PENIN, de limiter strictement l'action de la CSF dans les Télécommunications aux problèmes de détection (RADAR en particulier), aux transmissions par voie hertzienne et aux composants, tubes compris. Une illustration de cette position a été connue lors du projet de réalisation d'un émetteur-récepteur à 1 750 canaux, pour lequel le STTA avait mis en concurrence une PME, qui travaillait déjà sur des émetteurs moins ambitieux, et la CSF (usine de Levallois). Bien que l'appareil mis au point par cette dernière ait présenté de meilleures performances que celui de la PME, le STTA a décidé de confier la réalisation industrielle à cette PME. Enfin, il ne faut pas exclure que, d'une manière générale, le STTA n'était pas très favorable à la CSF.

Quant à la Marine, elle prétendait qu'elle était sur le point de présenter un prototype, mais la machine Ulysse rencontrait quelques difficultés techniques (sa mémoire était constituée de condensateurs) et seuls quelques exemplaires furent construits.

II.8. – LE CONCOURS INTERNE FRANÇAIS ET LA DÉCISION DU MINISTRE DE LA DÉFENSE.

Simultanément, se déroulait le concours interne français qui visait aussi à choisir une machine pour la France.

En effet, s'il y a un matériel de bureau très sophistiqué qui peut être commun à toutes les administrations françaises, c'est bien le matériel de chiffrement. Aussi, pour des questions de prix, lequel évidemment dépend évidemment des quantités à produire, le SCTI prend la décision de désigner une seule machine de cryptographie pour toutes les administrations. Sa décision s'appuiera sur l'avis technique du STCCh et, au point de vue financier, sur le prix auquel pourra être vendue une telle machine. Ce choix était aussi conditionné par l'obtention de l'approbation OTAN.

Comme nous l'avons vu, au début trois projets étaient en concurrence : la machine Myosotis de l'armée de Terre, la machine Violette de l'armée de l'Air, et la machine Ulysse de

la Marine. L'équipe d'évaluation du STCCh travaille essentiellement sur des données théoriques : ils effectuent une évaluation papier, à partir des données des constructeurs. Ces calculs concernent principalement le fonctionnement des registres et les périodes des machines. ANDRÉ vérifie que Violette est compatible avec la KL-7 et que sa version nationale est supérieure à la KL-7 (sa période est plus grande). Mais il trouve que la période de Myosotis est supérieure à celle de Violette. À la demande de MULLER, CATTIEUW fait une évaluation de la KL-7 et trouve qu'un mécanisme interne à la machine avait été conçu de façon optimale.

Mais, LLOPIS démontre que Ulysse présente des faiblesses théoriques : elle engendre des groupes (au sens mathématique du terme). Sa sécurité est donc jugée insuffisante par la sous-commission « Cryptologie ». Dans ces conditions et devant les difficultés techniques évoquées précédemment, cette dernière se retire assez vite de la compétition et le choix ne réside plus qu'entre Myosotis et Violette.

Le SCTI devait fixer son choix en fonction de trois critères : le prix, les qualités techniques et les qualités opérationnelles.

Pour comparer le prix des machines, le SCTI envoie aux deux sociétés concernées, CSF et SAGEM, une demande de prix pour une centaine de machines.

En fait, tant que l'industrialisation n'est pas faite, il est très difficile de fixer un prix. AMEIL fait le raisonnement suivant. Pour un matériel fabriqué en très grande quantité (téléviseurs, par exemple) le prix des matières premières peut représenter un pourcentage allant jusqu'à 80 % du prix de revient, mais pour une quantité n'exigeant pas des frais d'industrialisation importants, la part des matières premières se situe entre 30 et 50 %. Ne voulant pas interroger Levallois directement, il était difficile à Xavier AMEIL de donner une évaluation pertinente, mais il lui fallait répondre... Il obtint par l'équipe technique les éléments essentiels qui lui permirent de connaître, à peu près, le prix des matières premières. Puis il doubla à peu près ce prix pour obtenir le prix de revient, d'où le prix de vente, en tenant compte de la marge habituelle dans l'industrie des Télécommunications.

Pour être sûr de gagner la compétition financière, il alla voir l'ingénieur général CASAL qui lui fit comprendre que le prix envisagé était valable pour éliminer le concurrent au point de vue financier.

Restait à être aussi le premier au point de vue technique. Au début de l'étude, le chef du STCCh André MULLER n'était pas complètement acquis au projet de la CSF, mais petit à petit les démonstrations de l'équipe CSF, et en particulier de VASSEUR, l'ont convaincu que les possibilités techniques de Myosotis étaient supérieures à celles de Violette.

André MULLER et André CATTIEUW avaient examiné de près Violette. Ils avaient un bon dialogue avec la SAGEM. Il fallait donc les convaincre de faire un examen des études de GAUBERT et de VASSEUR. M. MULLER s'est montré attentif au nouveau « bébé » et a pris conscience de l'intérêt du projet CSF, et un climat de très bonnes relations s'instaura. Le tout premier projet que VASSEUR soumit à la sous-commission « Cryptologie » fut jugé insuffisant : la période était trop courte. VASSEUR présenta un second projet dont la période était cette fois suffisante. La mise à la clé qui consistait à enficher des permutateurs sur des connecteurs particuliers, était séduisante car elle offrait un très grand nombre de clés possibles ; mais le STCCh fit remarquer que tous les permutateurs n'avaient pas le même effet sur le calcul du crypto : la logique de Myosotis présentait une légère dissymétrie due à sa structure en couches successives, dont cependant l'avantage était de masquer vis-à-vis de la sortie les éléments les plus secrets. Mais VASSEUR trouva le remède à ce défaut : il proposa d'introduire un rebouclage dans la logique de Myosotis, rebouclage qui rendait symétrique le rôle des permutateurs. Finalement ce schéma fut adopté et ce fut la version finale de Myosotis ; à la suite de quoi MULLER décida de soutenir ce projet.

Par ailleurs, pour l'aspect opérationnel, il fallait également convaincre les utilisateurs futurs du produit, représenté essentiellement par le bureau « Chiffre » qui était tenu à ce moment-là par le colonel CULLMANN avec le commandant Félix RABAUD puis le colonel SAMSON. Ils furent assez vite

convaincus par ce que la CSF présentait. Ils considéraient que les conditions d'exploitation de la machine étaient très sensiblement plus simples que celles de Violette, mais aussi que la taille et le poids de Myosotis permettaient d'envisager un matériel tactique nécessaire à l'armée de Terre. *A contrario,* Violette était un matériel d'infrastructure dont le poids et l'encombrement permettaient son emploi sur les bases aériennes mais certainement pas à bord de « shelters » ou de véhicules militaires. Tous ces éléments ont participé à la prise de position du SCTI en faveur de Myosotis.

Cependant, sur le plan technique le choix restait difficile. La difficulté résultait d'une querelle d'experts au sein de la sous-commission « Cryptologie » de la Commission interministérielle des Chiffres, entre les tenants de Violette et les partisans de Myosotis. Querelle de cryptologues d'autant plus redoutable qu'on ne sait pas démontrer la valeur cryptologique d'un procédé de chiffrement... sinon en montrant qu'on sait le décrypter !!! et donc qu'il n'est pas bon ! Or, les sommités universitaires consultées, dont M. le professeur FORTET, pour arbitrer le débat se montraient fort prudentes devant l'enfer de complexité présenté par l'une et l'autre machine.

En plus de l'étude théorique et mathématique, la CSF avait produit une étude statistique très riche, ce qui n'avait jamais été fait à cette échelle, dans le monde des cryptologues français. La sous-commission était embarrassée pour donner un avis sur ce document [16]. Ce dernier a été évalué finalement par le principal conseiller scientifique du STTCh, le professeur BARRA.

Cette étude statistique a pesé dans le choix final de Myosotis. Mais le débat aura été tranché en prenant aussi en considération les aspects afférant à l'emploi : Violette, compatible avec la KL-7 dans un de ses modes de fonctionnement, apparaissait séduisante car pouvant s'insérer petit à petit dans les réseaux de chiffrement existants, tant nationaux que OTAN,

---

[16] Dans l'annexe IV nous donnons les raisons théoriques qui justifient un tel volume d'études statistiques. Mais ces raisons ne furent découvertes et comprises que plusieurs années plus tard.

mais la technologie utilisée (les thyratrons à cathode froide) conduisait à un matériel lourd et encombrant qui convenait uniquement pour des liaisons d'infrastructure, comme pour l'équipement des bases aériennes. Elle ne pouvait convenir aux liaisons tactiques de l'armée de Terre qui avait besoin d'un produit plus léger comme Myosotis.

Dans ces conditions, l'État-major des Armées, sur proposition du SCTI, donc de RIBADEAU DUMAS en tant que chef de la division « Transmissions et Chiffre » de l'EMA, décida que Myosotis serait la machine officielle dont devaient être équipées pour la cryptographie les trois armées. Les autres administrations, dont le ministère des Affaires étrangères, suivirent l'avis de la sous-commission et firent le même choix : Myosotis restait la seule machine à chiffrer pour la France.

Par ailleurs, le bloc de chiffrement, contenant toute la logique de Myosotis, fut classé « Diffusion restreinte » et son bloc de commande, qui contenait ses fonctions d'exploitation, ne fut pas classifié.

La décision officielle fut prise par le ministre de la Défense, M. Pierre MESSMER, en 1965.

Le gouvernement décida de récompenser les principaux acteurs de « l'opération Myosotis » : André MULLER remit les insignes de chevalier de la Légion d'honneur à Jean-Pierre VASSEUR en 1968 et à Xavier AMEIL en 1971.

TROISIÈME PARTIE

LA FABRICATION DE MYOSOTIS ET LA CRÉATION DE L'INDUSTRIE DU CHIFFRE EN FRANCE

III.1. – LE DÉVELOPPEMENT INDUSTRIEL ET COMMERCIAL DE MYOSOTIS.

L'aboutissement du projet Myosotis marquait une avance de la Thomson-CSF dans le domaine du Chiffre, non seulement sur le plan national mais aussi au plan international.

Mais à la suite du choix de Myosotis, SAGEM avait demandé une compensation. Dans le cadre d'un protocole d'accord suscité par le SCTI, il est décidé que SAGEM participera à la fabrication en série des Myosotis : SAGEM fabriquera le sous-ensemble de commande télégraphique, Thomson-CSF se réservant le bloc chiffrant.

En réalité, cette décision avait été anticipée par un compromis négocié par Roger AUBERT, directeur technique général de la CSF, et son homologue de la SAGEM. Par cet accord, AUBERT s'assurait que la machine Myosotis serait choisie et SAGEM, en acceptant ce choix, obtenait une fabrication de matériels et surtout conservait une place dans le domaine de la cryptographie. En fait, la SAGEM détenait le marché des claviers perforateurs-chiffrants (pour le ministère de l'Intérieur) et celui des TAREC (pour les Armées et le ministère des Affaires étrangères). Mais cela ne lui donnait guère de savoir-faire en matière de machine à chiffrer, d'autant qu'elle ne faisait rien, malgré les sollicitations du STCCh, concernant la production des bandes-clés associées aux TAREC, production qu'il fallait améliorer et moderniser !

Sur le long terme, ce calcul s'est révélé payant pour la SAGEM. En effet, même si la Thomson-CSF restait la première

pour la conception des matériels cryptographiques, la SAGEM réussit à s'introduire dans ce domaine en jouant la carte de la complémentarité, principalement autour de produits qui lui étaient propres (téléphones, téléimprimeurs...). Petit à petit, elle a renforcé son équipe de recherches en scientifiques et cryptologues (souvent avec l'aide du STCCh et même de la Thomson-CSF, entre autres par le biais des cours de cryptologie que le STCCh organisait et auxquels contribuaient les spécialistes de Thomson-CSF !). Et SAGEM est ainsi devenue le second fournisseur de matériels de chiffrement pour les administrations françaises.

Sans doute parce qu'il pressentait cela, Jean-Pierre VASSEUR ne fut pas du tout content de cet accord ! En effet, il pensait qu'il serait certainement difficile de faire vivre en France deux fabricants de matériels de chiffrement. Mais cette situation était, somme toute, plutôt confortable pour les administrations françaises qui pouvaient faire jouer la concurrence. Heureusement, une sorte de *modus vivendi* s'établit de fait entre les deux sociétés et la concurrence ne fut pas trop pernicieuse.

Il fallait maintenant organiser la fabrication industrielle des Myosotis. Il était évident que le laboratoire de RPC devait se retirer de cette affaire et qu'il fallait confier sa fabrication à une unité de la division « Matériels ».

Marc DUMAIRE quitte alors RPC en septembre 1966 pour transférer le laboratoire « Chiffre » sur le centre de Levallois où il regroupe l'équipe de SEIGNOL et SAMAIN qui avait assuré la réalisation des deux prototypes du concours OTAN depuis 1962.

Il ne reste à Puteaux qu'une petite équipe, sous la direction de VASSEUR, pour le prolongement des études de base, principalement mathématiques et informatiques, nécessaires à l'évolution des matériels, des composants et des besoins exprimés par les Armées et les administrations. D'ailleurs ces nouveaux besoins, suscités par les possibilités grandissantes de l'électronique devaient entraîner un flux d'études continu sur plusieurs années. Ceci incite rapidement Vasseur à renforcer son équipe en recrutant, fin janvier 1967, Gilles RUGGIU qui venait de

terminer son service militaire, en tant qu'affecté scientifique au STCCh où il avait eu l'occasion de s'initier à la cryptographie et aussi au problème des rayonnements compromettants [17].

Gilles RUGGIU, formé par Jean-Pierre VASSEUR, notamment en mettant la dernière main aux rapports techniques de Myosotis, sera rapidement chargé de la conception et de l'évaluation des nouvelles machines à chiffrer. Quelques années plus tard, Marc FOUGERES les rejoindra : il prendra en charge les aspects technologiques, qui sont alors en très forte évolution.

Pour la CSF, VASSEUR reste l'interlocuteur privilégié auprès des instances gouvernementales pour tout ce qui concerne le Chiffre.

Enfin la fabrication de Myosotis est confiée au centre de Cholet, rattaché à Levallois depuis sa création en 1936 (c'était, à l'époque, une usine de la SFR). L'usine de Cholet commence l'industrialisation de Myosotis en 1964 et sa fabrication en série en 1966. Elle était dotée d'un service d'étude et de développement. Une section de ce service prend en charge ce nouveau matériel, premier équipement numérique de l'usine, avec MM. CANDELIER et LAMOTTE qui avaient participé à l'étude et à la réalisation des prototypes à Puteaux et à Levallois.

Au début de la conception de Myosotis, les transistors au silicium ayant des performances suffisantes n'étaient pas disponibles. C'est pourquoi les transistors au germanium avaient été

---

[17] Le STCCh avait équipé son atelier du mont Valérien de cages de Faraday pour étudier les méthodes de mesure des rayonnements électromagnétiques. En outre, on s'inquiétait des rayonnements acoustiques que présentaient la plupart des machines à chiffrer et des terminaux électromécaniques. Le service allemand *Zentralstelle für das Chiffrierwesen* étudiait ce problème. Aussi Muller envoya-t-il Gilles RUGGIU en mission à Bad Godesberg pour se renseigner sur les résultats de leurs travaux. Ce service avait monté une impressionnante chambre sourde isolée (elle était suspendue) pour effectuer des mesures dans toutes les gammes de fréquences depuis les infrasons les plus bas, jusqu'aux ultrasons. Mais les résultats furent décevants car il était très difficile d'en extraire les informations sensibles, surtout avec l'introduction de l'électronique dans toutes ces machines.

choisis. Mais à l'époque du lancement de la fabrication des Myosotis à Cholet, les transistors au germanium commençaient à être supplantés par les transistors au silicium. Cependant l'usine de Cholet ne put prendre en compte cette évolution technologique : les délais de fabrication étaient trop courts et la reprise de la conception des Myosotis dans cette nouvelle technologie juste au moment de l'industrialisation aurait été trop coûteuse. C'est pourquoi la filière germanium fut maintenue pendant plusieurs années par l'usine de fabrication des semiconducteurs de la Thomson-CSF à Saint-Égrève.

Ce n'est que plus de vingt ans plus tard qu'une version au silicium (en circuit intégré à grande échelle : VLSI), beaucoup plus compacte et légère, fut fabriquée, sur une commande du ministère des Affaires étrangères.

Le développement de Myosotis fut une véritable révolution pour Cholet et Levallois. C'était à la fois la première réalisation d'un système numérique, le premier matériel à transistors et l'équipement le plus complexe jamais réalisé à Cholet. La machine comprenait environ 1 000 transistors et 4 000 diodes. Avant d'insérer les composants, il fallait percer 18 000 trous dans les cartes de circuits imprimés. Le problème du test final était aussi difficile à résoudre, pour une machine destinée à produire des caractères aléatoires. L'équipe de Cholet sut très bien résoudre tous ces problèmes. Les machines produites se sont avérées d'une grande fiabilité et les coûts de productions ont été bien maîtrisés puisque les prix de vente laissaient une marge confortable.

Le laboratoire « Chiffre » de Levallois devient une antenne avancée du centre de Cholet.

En 1968, à la suite de la fusion de la CSF et de la Thomson-Houston (qui s'appelait, en fait, la Compagnie Française Thomson-Houston-Hotchkiss-Brandt : CFTH-HB) pour constituer la Thomson-CSF, le laboratoire de Levallois fut transféré sur le centre DTC de Gennevilliers, l'usine de Cholet lui étant rattachée. En 1969, l'équipe de Jean-Pierre VASSEUR s'installa à Corbeville, au laboratoire central de recherches de la Thomson-CSF. À vrai dire, c'est contraint et forcé que ce

déménagement eut lieu, car le laboratoire de Puteaux devait être rasé pour laisser la place au boulevard circulaire de la Défense, quartier qui devait être entièrement rénové.

Désormais, les développements seront faits exclusivement à Gennevilliers, mais les études associeront toujours le LCR et Gennevilliers.

D'abord placé sous la responsabilité de DUMAIRE, le laboratoire « Chiffre » sera ensuite dirigé par Joël LEBIDOIS, dans le courant de 1975. Ce dernier, arrivé au laboratoire « Chiffre » à la mi-1974, venait de la Division « Faisceaux Hertziens » (DFH) où il avait eu un premier contact avec le Chiffre, à l'occasion de projets et de réalisations de réseaux hertziens sécurisés, en particulier pour l'exportation. C'est ce premier contact qui l'incitera à rejoindre le laboratoire « Chiffre ». À ce moment, DUMAIRE partit prendre la direction du service de micro-électronique à l'usine de Cholet.

Plus tard, Joël LEBIDOIS sera rejoint par Gérard CHRISTMANN en août 1974, arrivé comme stagiaire militaire, et embauché l'année suivante. Puis arrivèrent Dominique PONS et Gilles COLÉOU en 1979 et 1982 respectivement. C'est au sein du laboratoire « Chiffre » et en travaillant avec l'équipe de CORBEVILLE qu'ils se forment à la cryptologie. Et tous trois succéderont à LEBIDOIS, à la tête du laboratoire, respectivement en 1980, 1985 (CHRISTMANN étant appelé, cette année-là, à des fonctions commerciales) et 1987.

Entre-temps, en 1983, Gérard CHRISTMANN avait réuni les trois laboratoires : Parole, Chiffre et Guerre électronique, dans la même entité placée sous sa responsabilité, car le Chiffre jouait désormais un rôle pivot pour les deux autres techniques.

Devant le développement de cette activité, le laboratoire « Chiffre » devra renforcer son équipe commerciale. C'est d'abord le capitaine de vaisseau LAVOLLAY qui est embauché. Celui-ci est resté peu de temps car il devait rejoindre ensuite le STCCh en 1968 comme adjoint de M. MULLER pour les affaires générales. Mais Henri LAVOLLAY devait

décéder prématurément, en janvier 1971, des suites d'une longue maladie.

Cependant la société Thomson-CSF accroît son effort commercial pour le Chiffre. Cela est dû en particulier à François ROY, directeur commercial de la DTC durant les années 1970-1980. Celui-ci a beaucoup œuvré en faveur du Chiffre non seulement par son aide auprès des commerciaux propres au Chiffre mais aussi par son action personnelle auprès des grandes administrations militaires et civiles. Son souci était de conserver à la Thomson-CSF son monopole de la cryptologie militaire et gouvernementale car il considérait que c'était une pièce maîtresse pour la fourniture de moyens de transmissions. De plus, il savait faire valoir auprès des autorités françaises que la Thomson-CSF était leur meilleur atout dans ce domaine, grâce en particulier aux très bons rapports existant entre les équipes de la Thomson-CSF et les cryptologues des administrations.

Désireux de développer le Chiffre à l'exportation, François ROY fait venir, en 1973, Daniel DRONIOU, comme commercial export pour les matériels de chiffrement. Daniel DRONIOU était auparavant commercial du LCR à Corbeville. Mais les difficultés pour exporter ces matériels étaient énormes (voir le paragraphe suivant). Malgré cela, DRONIOU réussit quelques ventes des versions export du TRC 760 et du TRC 765. Cependant la version export du système Cyphon ne se vend pas. DRONIOU s'est aussi employé à équiper la gendarmerie. Il a occupé cette fonction jusqu'en 1982, année où il est nommé commercial de la DTC pour la zone Amérique latine.

Fin 1975, ROY embauche un nouveau commercial : le lieutenant-colonel Pierre BÉNAITEAU, ancien adjoint du chef du bureau « Chiffre » de la Direction centrale des transmissions et futur président de l'Association des Réservistes du Chiffre (ARC). Il restera le commercial principal du laboratoire jusqu'en 1988, quand il partira à la retraite. Cependant Pierre BÉNAITEAU s'installera à son compte comme ingénieur-conseil dans le domaine de la cryptologie et de la sécurité de l'information, et gardera, à ce titre, des relations étroites avec la Thomson-CSF.

III.2. – LA FOURNITURE DES MYOSOTIS ET LE PROBLÈME DE SON EXPORTATION.

En 1974, 1 000 machines auront été réalisées par Cholet et, au total, ce sont 1 500 équipements qui sortiront de l'usine de Cholet. Signalons que, grâce à l'habilitation OTAN, un ensemble de deux équipements (un pour chaque extrémité de la ligne) a même été fourni à la Norvège pour protéger une de ses liaisons !

Les trois armées et le ministère des Affaires étrangères se sont équipés de Myosotis.

L'armée de Terre, imitée par les Affaires étrangères, privilégie le chiffrement en ligne au sein de ses centres de transmissions et ses chiffreurs deviennent des crypto-télégraphistes. Par contre, l'armée de l'Air, son souci d'économie rejoignant son souci de sécurité, fait exploiter ses Myosotis hors ligne par des sous-officiers régulateurs chiffreurs.

Mais il faut noter que les marins et les aviateurs s'équipent aussi de matériels américains, dont la KW-7 et la KW-37 ! Cette dernière est une machine à chiffrer en ligne pour téléimprimeurs électroniques avec une vitesse maximale de 75 bits/s. Elle est d'un niveau de sécurité nettement inférieur à celui de la KW-7 (sa période, d'environ $5{,}4.10^9$, est cependant correcte), mais elle possède une fonction supplémentaire qui rend plus souple son utilisation : un mécanisme de rattrapage à 25 000 bits par seconde permet d'établir des transmissions en léger différé.

Caractéristique de cette évolution et de l'interpénétration du Chiffre et des Transmissions, provoquée par l'automatisation des opérations de chiffrement, l'instruction interministérielle 500/STCCh du 23 décembre 1968 officialise pour l'administration, à côté des centres ou ateliers de chiffrement qui subsistent, l'existence de centres de transmissions protégés. Elle officialise aussi les méthodes de chiffrement en circuit ainsi que le chiffrement de voie continu ou discontinu qui constituent un progrès considérable par rapport aux errements antérieurs. Les retards imputés au chiffrement disparaissent au prix, certes, d'un

investissement en matériels de chiffrement de coût élevé : une machine Myosotis avec son modem filaire coûtait 250 000 F en 1970.

Les ingénieurs d'armement et, en particulier, ceux de la SEFT et du SCTI, ont, tous, contribué au bon développement du Chiffre en France. Conscients de l'importance de l'enjeu que représente le matériel « Chiffre », leur préoccupation majeure était d'assurer aux Armées et aux autorités gouvernementales le meilleur Chiffre possible. Tout en sachant prendre en compte les contraintes économiques, ils n'ont jamais sacrifié la technique. Ils ont su faire confiance aux industriels et ont su leur éviter bien des difficultés, même si la tentation était forte de faire jouer la concurrence entre SAGEM et Thomson-CSF.

Il faut souligner l'action efficace du commandant TARIEL en faveur du développement industriel de Myosotis et des nouvelles applications (comme le fac-similé) qui ont immédiatement suivi son déploiement. En tant qu'ingénieur principal de l'armement, il avait suivi les cours du CECS de 1962 à 1964, en compagnie de André CATTIEUW et Georges ANDRÉ. Il faisait donc partie de la grande famille des « Chiffreurs » et nous pouvons dire qu'il a tenu le Chiffre à bout de bras au sein de la DMA. En cela, il a été remarquablement suivi par ses successeurs Alain FAUVET, puis Joël HOSATTE.

La grande affaire d'Alain FAUVET fut l'équipement Chiffre du RITA, le célèbre **R**éseau **I**ntégré des **T**ransmissions **A**utomatiques. Il conduisit ce projet avec le succès que l'on sait : le réseau RITA s'imposa comme un des meilleurs au monde grâce, en particulier, à l'efficacité et la facilité d'emploi de son Chiffre, parfaitement intégré à la fonction communication. Le RITA fut acheté par les E.-U. Lors des négociations de vente, les Américains exigèrent qu'on leur fournisse, dans le détail, tous les éléments de conception, de réalisation et d'évaluation du système de chiffrement, comme lors de l'évaluation de Myosotis dans le cadre du concours OTAN. La Thomson-CSF fut autorisée à les donner et les Américains les examinèrent de très près. Malheureusement, *in fine,* ils ne

prirent pas le système de chiffrement et équipèrent leur RITA d'un matériel américain [18].

Joël HOSATTE arriva à la SEFT en 1978. Il fut chargé, entre autres, du développement du Chiffre dans les liaisons par satellites (stations bord et sol). Le grand défi de ces projets était la vitesse de chiffrement qu'il fallait atteindre : les dizaines de millions de bits par seconde avec des puces qui devaient satisfaire toutes les contraintes du spatial : grande fiabilité attestée par des années d'expérience, résistance aux conditions physiques extrêmement sévères de l'environnement, ainsi qu'aux rayonnements. Ce fut l'occasion de développer les premiers algorithmes de chiffrement par blocs dont le prototype était le DES. Il conduisit aussi des travaux de cryptologie relatifs au réseau RITA, y compris pour l'export.

Enfin, Joël HOSATTE eut à gérer les nouveaux concepts du Chiffre à clé publique et les premières applications de ce qui allait devenir le chiffre civil. Il déclencha, dès son arrivée à la SEFT, en 1978, des travaux exploratoires sur ce sujet avec la Thomson-CSF, la SAGEM et l'Institut pour la Recherche en Informatique et Automatique (IRIA, Institut devenu par la suite Institut National : INRIA). Conscient de l'évolution que le Chiffre était en train de vivre, il relança, avec l'appui du SCCST, de nouvelles études théoriques de cryptologie.

Joël HOSATTE devait quitter la SEFT en 1983 pour le STEI (Service Technique de l'Électronique et de l'Informatique, créé au sein de la direction de l'électronique et de l'informatique). Mais cet éloignement ne dura pas trop longtemps, puisqu'il rejoignit le SCSSI en 1988, où il put se consacrer à nouveau au Chiffre jusqu'en 1993.

La grande question fut la fourniture de Myosotis aux pays étrangers qui n'étaient pas membres de l'OTAN. Il existait évidemment un marché qui, comme nous l'avons dit, intéressait la Thomson-CSF. Malheureusement, la France n'avait pas de politique d'exportation pour ce type de matériel, ni

[18] Certains diront : « Comme il fallait s'y attendre ! »

de crédits pour proposer une machine dérivée de Myosotis. En effet, il était clair qu'on ne pouvait la vendre telle quelle. Le STTCh avait demandé à la Thomson-CSF d'étudier une version de Myosotis pour l'exportation, mais celle-ci est restée dans les « cartons », faute de soutien politique et financier.

En fait, parler de la machine Myosotis ou la montrer à des personnalités de pays étrangers, à l'occasion de leur visite, amenait inéluctablement de la part de ces personnalités la question de l'exportation de ce matériel. Or, par ignorance des questions de sécurité nationale, les autorités françaises, au plus haut niveau, déclaraient souvent qu'il n'y avait pas de problème ; autrement dit, elles laissaient entendre que l'on pouvait leur en fournir. Mais ensuite, tout le monde était très ennuyé quand le pays faisait une demande d'achat de machines Myosotis, et personne ne savait comment répondre à cette demande.

Devant cette situation et par manque de politique d'exportation, le STCCh a demandé de cacher l'existence de Myosotis ! Les chiffreurs reçurent l'ordre de n'en pas parler et de considérer le nom même de Myosotis comme classifié [19].

Cet état de chose a, d'ailleurs, conduit à introduire les moyens de cryptologie dans le décret de 1973 régissant les matériels de guerre, et le STCCh à prôner une politique officielle d'exportation. Mais se posait alors le problème du financement des études du matériel destiné à l'exportation, financement que la Thomson-CSF ne pouvait supporter toute seule. Malgré les exhortations de STCCh, l'état-major, qui détenait les crédits militaires pour le matériel « Chiffre », soutenait que ce n'était pas son problème, son objectif étant d'équiper les forces ; et la Défense, de son côté, déclarait qu'elle mettrait son veto à toute demande d'exportation hors OTAN. Ce problème ne fut pas résolu et, plus tard, la même question s'est posée, sous une autre forme, avec le chiffre civil (cf. le paragraphe IV-5).

[19] Voir l'anecdote de La Nouvelle-Orléans de l'annexe III.

III.3. – LA COLLABORATION ENTRE LA THOMSON-CSF ET LES ADMINISTRATIONS.

La machine Myosotis a été conçue et étudiée par la CSF, mais en collaboration avec la DMA (devenue plus tard la DGA), le STCCh (aujourd'hui la DCSSI, Direction Centrale de la Sécurité des Systèmes d'Information, rattachée au secrétariat général de la Défense nationale) et la sous-commission « Cryptologie » de la Commission interministérielle des Chiffres.

Le succès du projet Myosotis est dû à l'excellente coopération des administrations, des industriels et des nombreux scientifiques qui ont assisté soit le STCCh, soit la CSF. Ces bons rapports n'empêchaient pas d'âpres discussions entre les différents spécialistes, discussions d'autant plus délicates que peu d'arguments étaient susceptibles d'être prouvés !

Outre ses propres experts et ceux de la sous-commission « Cryptologie », le STCCh avait de nombreux conseillers scientifiques, le plus souvent bénévoles. Les principaux d'entre eux furent : J. FAVARD, professeur à la faculté des sciences de Paris et à l'École Polytechnique ; Paul DUBREIL, professeur d'algèbre à l'université de Paris ; le professeur DUGUÉ, directeur de l'Institut supérieur de statistique de l'université de Paris, ainsi que le colonel Georges CULLMANN, ancien patron du bureau « Chiffre » de l'armée de Terre. Celui-ci avait rejoint la compagnie des machines Bull comme conseiller scientifique et était également professeur à l'École supérieure d'électricité.

Mais pour l'étude de Myosotis, le principal collaborateur scientifique du STCCh fut J. R. BARRA, professeur de statistique à l'université de Grenoble. Il avait conduit des études approfondies sur le contrôle statistique des suites aléatoires, en dehors de toute préoccupation cryptographique. Sous sa direction, plusieurs de ses étudiants, en particulier G. HISLEUR, avaient programmé un ensemble de tests portant sur le caractère aléatoire des suites. Ces programmes avaient été écrits en ALGOL 60 pour un calculateur IBM 7044. C'est J. R. BARRA qui établit les fondements de l'évaluation statistique des machines à chiffrer.

Le principal collaborateur scientifique de la CSF fut André BERROIR, professeur de mathématiques à l'université de Paris. André BERROIR contribua essentiellement à la théorie du fonctionnement de Myosotis. En concertation avec BARRA, il proposa beaucoup de tests et mis au point les lois théoriques servant de base à l'évaluation expérimentale. Il savait aussi tenir compte des aspects pratiques et concrets : c'est lui qui fixa les règles d'interprétation des résultats expérimentaux, interprétation très délicate eu égard à leur nombre.

Il faut aussi citer Pierre AIGRAIN qui marqua beaucoup d'intérêt pour ces travaux et pour le Chiffre en particulier.

C'est le grand mérite d'André MULLER, et aussi de Jean-Pierre VASSEUR, d'avoir su faire travailler ensemble toutes ces individualités, en bonne intelligence et estime réciproque. Jean-Pierre VASSEUR était invité régulièrement par André MULLER aux réunions de la sous-commission pour en recevoir les critiques et discuter des solutions.

MULLER entretenait un climat d'émulation et de franche amitié entre ses collaborateurs. Par ailleurs, il faisait le plus grand cas des « collaborateurs extérieurs » c'est-à-dire de ceux qui apportaient leur contribution au Chiffre, sans faire partie à proprement parler du STCCh. Ils étaient invités aux réunions soit en tant qu'utilisateurs comme membres des bureaux « Chiffre » des administrations, soit en tant que concepteurs comme industriels fabricants de matériels, soit en tant qu'évaluateurs, comme membres de la sous-commission « Cryptologie ».

Le dîner amical traditionnel que l'Association des Réservistes du Chiffre (ARC) organisait chaque année en janvier à Paris, constituait une bonne occasion de se retrouver tous ensemble dans une ambiance sympathique et joyeuse. L'ARC (devenue, en 1991, l'ARCSI, Association des Réservistes du Chiffre et de la Sécurité de l'Information) a maintenu cette tradition du dîner de janvier ouvert largement aux « collaborateurs extérieurs ».

MULLER organisait aussi, au printemps, des parties de campagne dans sa résidence secondaire à Gerberoy, dans l'Oise, où nous étions chaleureusement accueillis par madame MULLER.

Il faut souligner que les familles et, en particulier, les conjoints étaient invités. Comme il y avait beaucoup d'enfants, madame MULLER n'hésitait pas à transformer une chambre en nursery.

Les équipes de la Thomson-CSF et du STCCh ont continué à entretenir d'excellentes relations tout en poursuivant une fructueuse collaboration. Elles mirent au point ensemble de nombreux perfectionnements aux systèmes cryptographiques. Ces perfectionnements devaient profiter aux machines qui allaient succéder à Myosotis.

Cette collaboration s'est aussi concrétisée par la contribution des ingénieurs de la Thomson-CSF aux divers cours que le STCCh organisait pour ses stagiaires et auxquels la SAGEM apporta aussi sa contribution. Jean-Pierre VASSEUR participe à ces cours, dès 1972, essentiellement pour la cryptographie ; puis, à partir de 1974, Gilles RUGGIU apporte aussi son concours, pour la logique mathématique et l'informatique, et au début des années quatre-vingt, Marc FOUGÈRES pour l'électronique. Le laboratoire « Chiffre » de DTC apporta aussi sa contribution avec LEBIDOIS, CHRISTMANN, PONS, COLÉOU..., principalement pour les aspects systèmes, réseaux et technologies. Les stagiaires visitaient aussi les laboratoires et les usines de la Thomson-CSF et de la SAGEM.

Ces cours furent l'occasion pour Jean-Pierre. VASSEUR d'exposer ses idées dans un ouvrage qu'il intitula modestement : *Quelques réflexions pseudo-aléatoires sur le chiffre,* mais qui est resté interne à la Thomson-CSF (« Réservé Compagnie »). Cet ouvrage, rédigé en 1976, présentait les principes fondamentaux de conception et d'évaluation des machines à chiffrer ; il servait de base à Jean-Pierre VASSEUR pour les conférences qu'il dispensait aux stagiaires du STCCh. Lorsque VASSEUR arrêta ce cours en 1984, c'est Gilles RUGGIU qui le reprit, jusqu'en 1998.

III.4. – LE DÉVELOPPEMENT DES OUTILS D'ÉVALUATION DES MACHINES À CHIFFRER.

L'équipe de Jean-Pierre VASSEUR s'est dotée petit à petit d'outils nouveaux. Au début de l'évaluation de Myosotis, la sortie de la machine était perforée sur une bande qu'il fallait

dérouler manuellement. Jean-Pierre VASSEUR et Marc DUMAIRE comptaient à la main les figures faisant l'objet des tests. C'était long et pénible et, de plus, ils trouvaient rarement les mêmes résultats ! Aussi Jacques RIETHMÜLLER construisit-il une première machine de tests pour automatiser une partie de l'étude statistique expérimentale. Cette machine fournissait les fréquences brutes des figures observées. Les calculs étaient faits par VASSEUR à l'aide d'une petite machine électromécanique suédoise Facit (le modèle CM2-16), capable d'effectuer les calculs avec seize chiffres décimaux significatifs et sur laquelle il était devenu très rapide. Cette machine était munie d'un registre d'entrée, d'un totalisateur et d'un compteur, chacun comportant un index indiquant la position de la virgule. L'opération de base était l'addition, mais des leviers divers et une manivelle permettaient de réaliser automatiquement les quatre opérations arithmétiques. Beaucoup de courbes et d'abaques ont été construits pour faciliter les calculs.

Un grand progrès fut réalisé au début de 1967 grâce à l'acquisition d'une toute nouvelle machine : la Programma 101. Celle-ci permit enfin l'élimination de la tâche fastidieuse des calculs répétitifs. Véritable petit ordinateur personnel (c'était, en fait, le premier de ce type), cette machine, conçue et commercialisée par la société Olivetti, admettait aussi bien l'exécution directe, à partir du clavier, d'instructions (arithmétiques ou logiques) très évoluées, que l'exécution de programmes enregistrés et interprétés par le processeur. Sa mémoire principale, qui contenait les instructions et les données, était constituée d'un fil à magnétostriction, dans lequel circulaient en permanence les informations ; les registres pouvaient contenir des nombres allant jusqu'à 22 chiffres décimaux. La machine pouvait lire des cartes magnétiques qui servaient de mémoire secondaire, pour stocker les données ou les programmes. On pouvait inscrire un programme (et ses sous-programmes) sur plusieurs cartes magnétiques. Mais seules des portions de programmes limitées à 120 caractères (ou instructions, lesquelles étaient codées sur un caractère) pouvaient tenir dans la mémoire principale. Le grand avantage de cette machine était son utilisation interactive et la facilité d'introduction des données. C'est Gilles RUGGIU qui fut

chargé de la programmer. Il faut dire que la programmation de la Programma 101 était très acrobatique, en raison de la petite taille de sa mémoire. Il fallut recourir à de nombreuses « astuces » de programmation pour tout faire tenir dans la mémoire. Ce fut les premiers programmes d'analyse statistique cryptographique réalisés à Thomson-CSF et appliqués à une machine à chiffrer. Beaucoup d'autres allaient suivre. Mais peu après la Programma est supplantée par le système APL de l'IBM 1130, machine que venait d'acquérir l'équipe de Jean-Pierre VASSEUR. Ce système conversationnel s'est révélé idéalement adapté à ce type de programmes.

Vers la fin de l'année 1968, une machine de tests plus complète et plus rapide que la précédente est réalisée : elle est baptisée APREDOSTAT, acronyme de « APpareil de REcueil de DOnnées STATistiques ». Cette machine, conçue par VASSEUR, RIETHMÜLLER et RUGGIU, a permis de gagner plus d'un facteur dix dans la durée des travaux d'évaluation statistique tout en simplifiant beaucoup les procédures de tests, grâce à son automatisation et sa grande facilité de programmation. En outre, elle permettait de réaliser de nouvelles mesures sur un plus grand nombre de données. Construite d'une façon modulaire, on put lui adjoindre de nouveaux sous-ensembles pour réaliser de nouveaux types de tests. Beaucoup de commandes de l'APREDOSTAT étaient automatisées, mais elles exigeaient encore l'emploi de maquettes adaptées pour étudier les nouvelles machines à chiffrer.

Un double de l'APREDOSTAT fut construit pour le STTCh. Cette machine lui permit d'être en mesure d'effectuer lui-même les mesures réelles sur les machines à chiffrer, et donc de conduire une évaluation expérimentale.

L'APREDOSTAT permettait d'analyser les suites de clés ou les cryptogrammes produits par les machines à chiffrer en recherchant des corrélations ou des figures particulières. Comme en général les machines produisaient plusieurs suites en parallèles, que l'on appelait pistes, il pouvait traiter jusqu'à cinq pistes simultanément. Il comportait une horloge, des registres, des détecteurs et des compteurs programmables.

Cette machine devait pouvoir s'adapter à toutes sortes de machines à chiffrer qui pouvaient avoir des caractéristiques très différentes selon le type d'application : télégraphie, fac-similé, phonie, images... C'est pourquoi l'horloge était programmable et pouvait fonctionner depuis les fréquences les plus basses jusqu'à plus de 10 MHz. Les compteurs et les registres à décalage étaient en technologie TTL [20] ou T2L (la toute nouvelle série 74 de Texas Instruments). En outre, les détecteurs et les compteurs étaient programmables par un jeu de câbles et de boutons. La structure des registres était aussi modifiable.

Les compteurs étaient composés de décades de type Johnson, qui demandaient cinq bascules au lieu des quatre habituelles, mais qui avaient l'avantage que leurs dix états se décodaient très facilement, sans impulsions parasites. Chaque décade comportait donc cinq bascules du type « J-K flip-flop » 7470 et les portes nécessaires au rebouclage et au décodage des états, sans possibilité de modes parasites. La taille des compteurs était impressionnante pour l'époque : ils permettaient de compter des longueurs de suites pouvant atteindre 10^7.

Les registres étaient constitués de bascules D, à raison de deux bascules par boîtier. Les cartes étaient de dimensions modestes (de l'ordre de 20 cm de côté), mais nombreuses de sorte que l'APREDOSTAT était assez imposant : près de 2 m de haut sur 70 cm de large et de profondeur. Malgré son étendue, l'appareil fonctionnait correctement à des fréquences dépassant 10 MHz, ce qui fut pour nous une agréable surprise, car nous faisions notre apprentissage en l'usage des circuits TTL.

Cette machine, cependant, exigeait encore la construction de maquettes spécifiques et beaucoup de manipulations pour étudier les nouvelles machines à chiffrer. Cet inconvénient commença à être fortement ressenti lorsque ces nouvelles

---

[20] Transistor-Transistor Logic, famille de circuits intégrés à transistors bipolaires.

machines furent plus souples d'emploi que l'APREDOSTAT lui-même. Ce fut notamment le cas avec les dispositifs de mise à la clé que permettaient les nouveaux circuits électroniques. Mais la construction d'un APREDOSTAT plus évolué ne fut pas envisagée, car celui-ci serait devenu trop complexe. En fait, il fallut attendre encore une dizaine d'années que les ordinateurs deviennent assez puissants pour pouvoir remplacer l'APREDOSTAT par un logiciel.

QUATRIÈME PARTIE

LES MACHINES POSTÉRIEURES À MYOSOTIS ET LE DÉBUT DU CHIFFRE CIVIL EN FRANCE

IV.1. – LES CONSÉQUENCES SCIENTIFIQUES ET INDUSTRIELLES DU PROJET MYOSOTIS.

Le projet Myosotis a permis de fixer la doctrine française de conception et d'évaluation des machines à chiffrer. Ce sont les travaux d'analyse et d'évaluation de Myosotis qui ont donné une base scientifique à cette doctrine. Celle-ci a d'ailleurs été validée par l'évaluation positive qu'en a faite l'agence alliée d'évaluation cryptologique (SECAN) et on s'apercevra d'ailleurs que Myosotis n'avait rien à envier aux matériels équivalents tels que l'ELCROTEL allemand, la KW-7 américaine ou l'ALVIS britannique.

En effet, c'est en s'appuyant sur les travaux de SHANNON et sur l'expérience pragmatique des cryptologues et des chiffreurs, qu'ont été fixées les bases du savoir-faire en matière de conception algorithmique de la logique fondamentale des machines à chiffrer et de prise en compte des contraintes d'utilisation ; par exemple un responsable d'exploitation comme Félix RABAUD a su définir les caractéristiques du trafic télégraphique, les procédures de prises de contact, les modes d'exploitation, en ligne ou hors ligne avec 26, 31 ou 32 caractères.

Par ailleurs, sont étudiées et mises en œuvre, sous l'égide du STCCh, les méthodes et procédures d'analyse et d'évaluation des machines à chiffrer, d'une part au plan cryptologique et d'autre part au plan des rayonnements compromettants (TEMPEST).

Ce dernier sujet constituait un domaine nouveau, les mesures correspondantes pour vérifier la conformité aux normes firent

l'objet de nombreux examens. Au début aucune norme n'existait en matière de rayonnements compromettants : aucune règle ne précisait les conditions de mesure. Il a fallu s'équiper de matériels spéciaux et très sophistiqués pour dégager des principes. La CSF se constitue alors assez vite un savoir-faire relatif aux rayonnements compromettants, tant en ce qui concerne les filtres que les règles de câblage et de blindage. Petit à petit une doctrine en matière d'évaluation et d'installation des ensembles cryptographiques concernant l'aspect TEMPEST finit par être agréée.

Cette doctrine a été concrétisée par l'instruction interministérielle sur les rayonnements compromettants et les règles techniques de sécurité des matériels des communications 300/STCCh du 7 avril 1973.

La Thomson-CSF mais aussi la SAGEM acquièrent, de fait, une grande compétence dans la mesure, l'analyse et la maîtrise de ces rayonnements compromettants.

De nouvelles techniques mathématiques, dérivées des mathématiques discrètes (groupes et corps finis, algèbres de BOOLE, théorie des codes et des automates, processus récurrents et chaînes de MARKOV, complexité algorithmique...) ont été progressivement développées et adaptées au cas des machines à chiffrer dont la principale caractéristique est le grand nombre de variables couplées. Le recours à ces nouvelles méthodes mathématiques était devenu indispensable dans la mesure où la complexité de Myosotis (et des machines suivantes) ne permettait plus une analyse cryptologique traditionnelle. Elles ont aussi permis de tirer le plus grand profit des nouveaux circuits intégrés : registres à décalage, mémoires RAM ou ROM, statiques ou dynamiques...

De même, de nouvelles méthodes et procédures statistiques ont été mises au point. Ces méthodes pouvaient être appliquées soit à la conception et à l'évaluation des matériels, soit à l'attaque des machines (décryptements). Il faut dire que c'est grâce à l'introduction progressive de la programmation que ces nouvelles techniques algébriques ou statistiques sont devenues applicables dans des temps et avec des moyens raisonnables.

Tout système de chiffrement doit comporter un générateur d'aléa. Les premiers dispositifs de ce genre que nous avons construits étaient basés sur le bruit de fond d'un transistor. Celui-ci était amplifié à un niveau convenable par un amplificateur à large bande, aussi à transistors. La sortie était échantillonnée par une impulsion très fine à une cadence très inférieure à la bande passante de l'amplificateur. Ce générateur de bruit était soigneusement blindé pour préserver la qualité de l'aléa. Malgré ce blindage, l'ensemble tenait sur une carte.

C'est à cette occasion que l'on s'aperçut que le bruit naturel obtenu de cette façon est loin d'être aléatoire. Celui-ci présente toujours un biais systématique dû à l'existence d'états préférentiels des circuits électroniques : par exemple pour discriminer les états 0 et 1, la précision du comparateur, réglé au niveau 0,5, ne peut assurer une équiprobabilité des niveaux 0 et 1, en raison de l'imprécision inévitable du comparateur. Le défaut d'équiprobabilité atteint facilement 10^{-4}. En outre ces mécanismes sont assez sensibles à la température : le défaut d'équiprobabilité peut doubler pour un accroissement de la température de 50 ^{0}C.

Pour y remédier, plusieurs dispositifs simples, comme le correcteur de von NEUMANN (décrit dans l'annexe IV-5), pouvaient être employés. Mais ceux-ci présentaient de nombreux inconvénients pour l'usage que nous devions en faire, en particulier l'irrégularité de la sortie. Finalement la meilleure solution que nous ayons trouvée était de transformer la sortie du générateur d'aléa par la machine à chiffrer elle-même (ou une partie de celle-ci). Cette transformation permettait d'obtenir cette équiprobabilité et toutes les propriétés dont nous avions besoin. Par un curieux retournement des choses, c'était une machine parfaitement déterministe qui nous fournissait le véritable aléa ! En revanche, le générateur de bruit physique garantissait l'imprévisibilité à moyen et long termes de la suite de bits obtenue.

Ce fut l'occasion pour l'équipe de Jean-Pierre VASSEUR et, en particulier, pour Gilles RUGGIU de réfléchir sur le concept

de nombres ou de suites aléatoires. Cette notion était encore peu claire au début des années soixante. Il y avait bien eu, dès les années trente, les travaux de von MISES. Puis, au cours des années soixante, KOLMOGOROFF avait émis l'idée de rattacher la notion d'aléa à la toute nouvelle théorie de la complexité des algorithmes (que nous présentons brièvement dans l'annexe I, paragraphe 7). Cependant, c'est G. CHAITIN qui, au début des années soixante-dix, en donna un éclairage nouveau et décisif pour la compréhension de cette notion (cf. l'annexe IV, paragraphe 3), dans le cadre d'une théorie simple et très intuitive.

La conclusion la plus frappante de CHAITIN rejoignait une intuition que nous avions tous et qui peut se résumer ainsi : *« Le caractère aléatoire des nombres (ou des suites) est indécidable. »*

Mais la théorie de CHAITIN, grâce à une définition acceptable de la notion d'aléa, fournissait une preuve de cet énoncé ! Cette théorie permit aussi de trouver des limites à l'étude statistique des machines à chiffrer : on comprit clairement la complémentarité de l'étude statistique d'une part et de l'analyse mathématique d'autre part, laquelle tendait de plus en plus à se subdiviser en deux aspects différents : l'aspect algébrique et l'aspect algorithmique.

Se basant sur les principes de conception qu'elle maîtrise parfaitement, l'équipe de Jean-Pierre. VASSEUR, avec essentiellement Gilles RUGGIU, puis avec Marc FOUGÈRES, commence à automatiser certaines étapes de l'étude mathématique grâce à des logiciels, réalisés d'abord sur IBM 1130, puis sur 370. Beaucoup ont été écrits en APL (sigle de : A Programming Langage), le puissant langage de programmation conçu par K. IVERSON (IBM Fellow) et A. FALKOFF.

Certains programmes ont même été écrits pour la machine IBM 5100, le tout premier ordinateur personnel fonctionnant entièrement en APL (le langage BASIC était aussi disponible sur cette machine). C'était nouveau à cette époque où les ordinateurs étaient confinés dans des salles climatisées et où seuls des opérateurs qualifiés avaient le droit d'y toucher. L'intérêt

de pouvoir travailler sur un ordinateur personnel avait été tout de suite perçu par Jean-Pierre VASSEUR : il avait acheté la 5100 directement aux États-Unis, au grand étonnement de IBM France qui ne la connaissait pas encore ! Mais elle fonctionnait en 60 Hz et nous n'avions pas osé la brancher sur le secteur à 50 Hz, IBM n'assurant dans ce cas aucune garantie. Finalement, Marc FOUGÈRES a construit un énorme onduleur qui fournissait le 60 Hz nécessaire !

La 5100 tenait sur le bureau de son utilisateur et les calculs étaient affichés sur un petit écran. Sa mémoire de masse était une bande magnétique amovible et elle était connectable à une imprimante. Nous nous étions aperçus que les circuits de l'affichage sur l'écran rayonnaient fortement, de sorte qu'un récepteur assez simple permettait de reproduire l'écran à quelques dizaines de mètres. FOUGÈRES avait monté une manipulation pour vérifier les possibilités d'interception qui en résultaient. Nous en avons fait une démonstration aux experts de STCCh qui ont été très impressionnés : c'était la première interception (en France, du moins) de rayonnements électromagnétiques émanant de matériels informatiques. On fit très rapidement des démonstrations analogues avec des consoles de visualisation alphanumériques qui étaient beaucoup plus courantes à l'époque.

D'abord destinés à vérifier ou à résoudre certains aspects particuliers du fonctionnement des machines à chiffrer, ces logiciels sont ensuite devenus des outils d'aide à la conception de ces machines et pouvaient même construire automatiquement certaines de leurs sous-fonctions.

Enfin, au début des années quatre-vingt, avec l'apparition des premiers PC (Personal Computer) qui commençaient à offrir des performances acceptables (grâce aux microprocesseurs INTEL 80186), ces outils ont été portés sur PC, ainsi que les tests statistiques. Ainsi fut constituée par Marc FOUGÈRES une boîte à outils très complète, quoique toujours en évolution, réduisant enfin l'APREDOSTAT en logiciel. En effet, il fallait profiter des progrès de la technologie mais aussi des avancées théoriques qui accompagnaient le développement des nouvelles

machines pour améliorer et enrichir ces outils. Si bien que l'étude, la conception et l'évaluation pouvaient se faire entièrement par simulation, rendant inutile la réalisation de maquettes. Pour rester dans des temps raisonnables, il fallait cependant faire travailler au moins quatre ou cinq PC en parallèle pendant plusieurs semaines ! D'ailleurs, pour des raisons d'efficacité, beaucoup de ces programmes, écrits à l'origine en APL, ont été ensuite traduits en Pascal ou en Fortran.

Si les bases théoriques et scientifiques de la cryptologie (mathématiques, statistiques et algorithmiques) sont bien connues au STCCh, en fait l'application industrielle de toutes ces connaissances et les outils de mise en œuvre sont essentiellement maîtrisés par la Thomson-CSF et l'équipe de Jean-Pierre VASSEUR. Celle-ci a, en outre, accès aux derniers développements des technologies électroniques et sait en tirer le meilleur parti pour optimiser la logique et le fonctionnement des machines à chiffrer. Or, ces technologies sont déjà en pleine évolution avec le développement des premiers circuits intégrés, d'abord en T2L, puis en MOS et en CMOS.

On peut dire que seule la Thomson-CSF, en tant que fabricant industriel, est, à cette époque, en mesure de concevoir les nouvelles machines à chiffrer dont la France va avoir besoin. Sa maîtrise de la conception des machines à chiffrer et des technologies de l'électronique lui permettait de répondre très rapidement aux demandes des autorités gouvernementales.

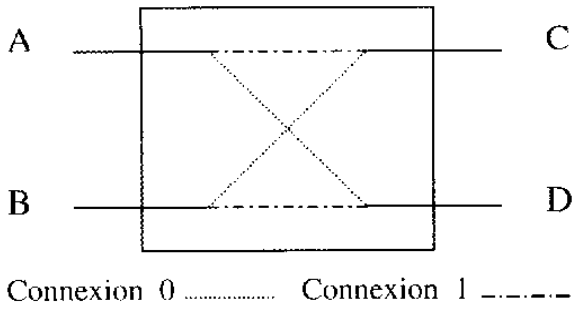
À partir de la spécification du besoin : caractéristiques du trafic (vitesse, tailles et types de messages...) et modes d'exploitation (en ligne ou hors ligne, en réseau, chiffrement d'artères ou de bout en bout, intégration dans les systèmes, gestion et distribution des clés...), l'équipe de VASSEUR, associée aux équipes de développement de Gennevilliers, pouvait définir très rapidement les principaux paramètres dimensionnant la machine, la technologie à choisir, la structure générale de la machine et sa logique de commande. Par simulation, une première étude de la logique de la machine pouvait être immédiatement lancée, ainsi qu'une première estimation des circuits nécessaires et des performances attendues.

IV.2. – LA MISE À LA CLÉ ÉLECTRONIQUE.

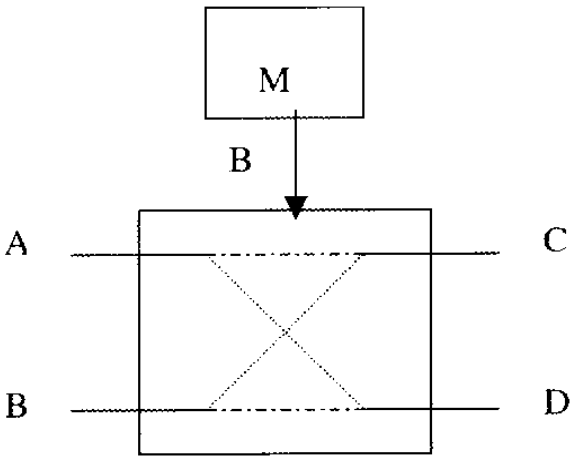
Cependant la mise à la clé de Myosotis restait manuelle. Même si celle-ci, grâce aux permutateurs enfichables, était beaucoup plus aisée que celle des machines précédentes, comme l'Enigma, la mise en place de ces permutateurs demandait tout de même un travail délicat et complexe. Aussi, VASSEUR se mit-il aussitôt à chercher une solution électronique susceptible de grandement simplifier la mise à la clé. L'arrivée des premiers circuits intégrés à grande échelle (LSI) lui permit de mettre au point une solution très élégante.

Les transistors en technologies MOS se prêtent très bien à la réalisation de circuits de commutation. Or, un permutateur binaire commute deux fils électriques : si ses entrées sont A et B, et ses sorties C et D, il peut soit relier A à C et B à D, soit A à D et B à C. Il a donc deux états distincts.

Le schéma ci-contre représente un permutateur binaire où un état (disons l'état 0) établit les connexions selon les connexions 0 et l'état 1 selon les connexions 1.



VASSEUR proposa de remplacer les permutateurs câblés par des permutateurs électroniques, les deux états de chaque permutateur binaire étant définis par une information binaire B prélevée dans une mémoire M, comme ci-contre :



La mise à la clé de la machine à chiffrer consistait simplement à charger dans la mémoire ces bits d'information par un mécanisme de transfert opérant soit à partir d'une mémoire extérieure contenant la clé du jour, soit à partir d'un clavier sur lequel on pouvait la taper. Une machine à chiffrer étant constituée de mémoires sous forme de registres à décalage, ce dispositif était très simple à réaliser et peu coûteux. En outre, il prenait peu de place et était très léger. Une telle solution s'imposait donc pour les matériels portatifs : les permutateurs électroniques binaires ont été utilisés pour la première fois dans les matériels de crytophonie numériques tactiques. Désormais la machine était entièrement électronique : un pas considérable était ainsi franchi.

Cependant un problème théorique et pratique se posa immédiatement : en réalité, au sein d'une machine on doit commuter N fils et non pas seulement deux fils. Comment réaliser un permutateur d'ordre N à partir d'informations binaires et possédant toujours toutes les propriétés désirées ? Ce problème était déjà très étudié par les concepteurs des centraux téléphoniques, dont la fonction principale est de commuter les abonnés désirant communiquer entre eux. À partir de 1964, plusieurs publications, dues pour l'essentiel à V. E. BENES [21] des *Bell Telephone Laboratories*, donnaient les bases de la solution.

Ces travaux présentaient des solutions pour construire, de manière récursive, des permutateurs d'ordre N à partir de permutateurs plus petits : un permutateur d'ordre $N = M \times P$ (ce qui suppose que N n'est pas un nombre premier), s'obtient en combinant des permutateurs d'ordre M et des permutateurs d'ordre P. Ces résultats sont des conséquences directes de théorèmes généraux sur la décomposition des groupes (l'ensemble des N ! (factorielle N) permutations d'ordre N forme un groupe). Quand N est une puissance de 2 : $N = 2^q$,

[21] Voir, par exemple, V. E. BENES, « Permutation Groups, Complexes, and Rearrangeable Connecting Networks », *The Bell System Technical Journal*, vol. 43, juillet 1964, pp. 1619-1640.

le permutateur d'ordre N est entièrement construit à partir de permutateurs binaires. Les réseaux obtenus de cette façon sont appelés « réseaux de Clos ».

Ces réseaux étant inversibles, il est très commode de les utiliser dans les circuits de calcul du cryptogramme. Cependant la complexité de réalisation de ces réseaux croît d'une façon exponentielle avec l'ordre N des permutations ; si N est grand, on ne peut réaliser qu'une sous-famille restreinte du groupe des permutations. C'est en particulier le cas pour les algorithmes de chiffrement par blocs (de 16, 32 ou 64 bits), où pour compenser la petite taille de la sous-famille des permutations, on itère plusieurs fois une transformation de base, tirée de cette sous-famille. Il est clair que la sous-famille doit être choisie soigneusement afin d'éviter les complexités illusoires. Ce type de structure est aujourd'hui au cœur des algorithmes de chiffrement par blocs.

C'est ce type de réseaux que VASSEUR proposa d'utiliser. Il fallait cependant s'assurer que ces circuits présentaient de bonnes propriétés cryptographiques. Des études, réalisées essentiellement par VASSEUR et RUGGIU, permirent d'établir les conditions d'utilisation optimale de ces réseaux ainsi que leurs caractéristiques du point de vue cryptographique. Ces propriétés se révélèrent très intéressantes et, par la suite, ces réseaux furent largement utilisés dans la conception des nouvelles machines à chiffrer.

Une dizaine d'années plus tard, IBM publia un nouveau système de chiffrement : Lucifer. On sait que ce système est à l'origine du système de chiffrement DES normalisé par le NBS (cf. l'annexe I, paragraphe 5). On s'aperçut que Lucifer faisait aussi appel à ce type de réseaux, qui furent appelés « schémas de Feistel », du nom du principal concepteur de Lucifer [22].

---

[22] En fait, il y eut plusieurs variantes de ces schémas, si bien qu'aujourd'hui l'expression « schéma de Feistel » désigne plusieurs types de réseaux, quelquefois assez différents les uns des autres. Mais ce sont toujours des réseaux de permutations particuliers.

IV.3. – LA CONTROVERSE « MACHINE À CÂBLAGE VARIABLE » VERSUS « MACHINE À CÂBLAGE FIXE ».

Les permutateurs de Myosotis ont deux fonctions :

- certains définissent l'état initial de certaines mémoires de la machine ;
- les autres définissent une partie du câblage interne de la machine.

Les premiers permutateurs ne sont actifs qu'à l'initialisation de la machine. Ils n'ont plus de rôle en cours de fonctionnement. Les seconds déterminent la structure de la machine qui reste fixe pendant toute une crypto-période. L'analyse cryptographique tenait compte de ces fonctions et toutes les formules de calcul étaient adaptées à cette façon de voir les choses. Ce point de vue n'était pas remis en cause avec les permutateurs électroniques.

Cependant VASSEUR se rendit compte que cette nouvelle conception revenait à laisser fixe pendant toute une crypto-période un grand nombre de mémoires internes de la machine qui donc ne contribuaient pas à sa variabilité. Or, du point de vue de l'électronique, les permutateurs pouvaient changer d'état comme n'importe quel élément de la mémoire de la machine. C'est pourquoi Jean-Pierre VASSEUR proposa donc de les faire varier au même titre que les autres mémoires de la machine. Ceci augmentait considérablement la complexité de la machine. Mais alors les principes précédents d'analyse et de calculs ne s'appliquaient plus de la même façon à une telle machine. Comment étudier ce type de machine ? Ceci fut le début d'une nouvelle controverse entre cryptologues, controverse qui dura quelques années !

Étudier une machine à chiffrer revient à analyser son graphe de changement d'état. Celui-ci est si complexe qu'on ne peut le calculer et on n'en obtient qu'une représentation très approximative que l'on appelait d'une façon très suggestive, due à J. FAVARD, « le champ de patates de la machine ». Cette appellation provient du fait que le graphe de la machine se décompose en composantes connexes qui ressemblent à des patates ! Et une machine est d'autant meilleure que d'une part

son « champ de patates » contient beaucoup de « patates » et, d'autre part, que ces « patates » sont grandes, c'est-à-dire contiennent beaucoup d'états ! Ceci est dû au fait que si beaucoup de messages sont chiffrés alors que les états de la machine sont sur la même « patate », la probabilité de produire des messages parallèles est d'autant plus grande que la patate est petite, mettant en cause la sécurité du chiffrement (voir l'annexe II, paragraphe 3.2).

Or, une machine dont le câblage est variable possède autant de « champs de patates » distincts que de clés tandis qu'une machine à câblage fixe ne possède qu'un seul « champ de patates ». Et les calculs montrent que pour une complexité équivalente, c'est-à-dire pour un même nombre d'états internes et une longueur des clés équivalente, une machine à câblage variable possède au total beaucoup plus de patates qu'une machine à câblage fixe. Dans ces conditions les risques de produire des messages parallèles pouvaient devenir sérieux. Il fut nécessaire d'approfondir les calculs relatifs au recouvrement de clés pour mieux estimer le danger !

Heureusement les progrès de l'électronique allaient très vite et trois facteurs jouèrent en faveur des machines à câblage fixe.

• Les circuits en LSI permirent d'augmenter à très peu de frais la période du moteur ; ceci permit d'obtenir des probabilités de recouvrement de clés extrêmement faibles.

• L'amélioration des techniques d'initialisation des machines permit de mieux faire jouer un rôle symétrique à l'ensemble des circuits internes ; ainsi les différents états se trouvant sur la même « patate » étaient équivalents.

• L'évolution vers le chiffrement par blocs, devenue possible grâce à la vitesse et au parallélisme des circuits, permettait d'augmenter la taille des alphabets de chiffrement. Le nombre dangereux de messages parallèles devenait très grand, et la probabilité d'atteindre ce nombre pouvait être rendue extrêmement faible, voire négligeable.

Finalement le débat fut tranché en faveur des machines à câblage fixe. Et, à partir de la CNT (voir le paragraphe suivant), la structure de toutes les machines à chiffrer fut de ce type.

IV.4. – LES ÉTUDES POSTÉRIEURES À MYOSOTIS.

Tout ce savoir-faire, fondamental, bâti à l'occasion des études de conception et de réalisation de Myosotis va servir pour les études des produits ultérieurs.

En effet, très rapidement, les Armées financent et entretiennent un flot constant d'études et de réalisations pilotées par la DGA en fonction des besoins exprimés par les différentes Armées au sein de la *« sous-commission « Chiffre » de la Commission interarmées des transmissions de l'électronique et du chiffre »* animée par la division « Transmissions » de l'État-major des Armées. Certaines administrations civiles commandent aussi des études de machines à chiffrer. Ces études sont suffisantes pour soutenir, avec la Thomson-CSF, mais aussi la SAGEM, une industrie française du Chiffre indépendante, capable de satisfaire les besoins gouvernementaux sans recourir aux produits plus ou moins douteux du marché international. Des études théoriques à caractère fondamental sont même passées au groupement Thomson-CSF/SAGEM, constitué en consortium pour l'occasion. Il faut dire qu'à ce moment, dans le domaine du Chiffre, il n'y a plus beaucoup de concurrence entre les spécialistes de ces deux sociétés qui s'apprécient mutuellement.

Les besoins des départements civils sont exprimés au niveau interministériel au sein de la sous-commission « Cryptologie » où ils sont souvent pris en compte par les militaires.

Sans être exhaustif, on peut citer les principales réalisations suivantes.

a) La CNT (Cryptophonie Numérique Tactique) en technologie MOS fonctionnant en modulation delta (à 16 kbits/s) et adaptée aux postes radio portatifs TRPP-13, fabriqués à Cholet sous licence américaine. Son étude avait été commencée en 1968 à Puteaux, puis s'était poursuivie à Corbeville. Le premier problème était de trouver une modulation numérique de qualité suffisante et qui puisse se satisfaire de la bande assez étroite du TRPP-13, lequel n'avait pas été conçu pour cela. Différents systèmes ont été réalisés et essayés sur le terrain, principalement par Jacques RIETHMÜLLER (PCM, Delta, et

hybrides entre les deux, Delta adaptative). La modulation Delta simple a finalement été retenue. Ce n'était pas le meilleur système quand la liaison était bonne mais c'était celui qui donnait la meilleure compréhension en limite de portée.

D'autre part, il fallait faire une machine portable, ce qui n'était pas le cas de Myosotis avec ses transistors discrets. VASSEUR choisit la technologie qui lui paraissait la plus prometteuse quant à ses capacités d'intégration : la technologie MOS dynamique [23] sur silicium. Au début de l'étude, on savait intégrer 10 transistors MOS sur une puce. VASSEUR fit le pari qu'à la fin de l'étude, on saurait intégrer 100 à 200 transistors ; finalement la machine a été réalisée avec des puces ayant plus de 300 transistors. C'est Jean-Pierre MOREAU qui, en coopération avec SEIGNOL, réalisa la conception de ces puces. Peu après, Jean-Pierre MOREAU devait rejoindre l'usine de Saint-Égrève pour développer la filière MOS. Ceci a conduit à une clé dont la logique était très différente de celle de Myosotis et qui a dû faire l'objet d'une évaluation particulière.

Un des problèmes difficiles de la CNT était la prise de contact. Il fallait transmettre sans erreur des conditions initiales, puis faire démarrer les deux clés d'émission et de réception exactement au même moment, à un bit près ! Nous avons ainsi défini une procédure de démarrage extrêmement redondante et qui s'est avérée très efficace (c'est ce que l'on a appelé des « bits lourds [24] », un bit étant remplacé par cent bits). En pratique, la liaison était très souvent parasitée et il arrivait que la conversation fût incompréhensible alors que la prise de contact avait été correcte.

---

[23] MOS signifie Métal-Oxyde-Semi-conducteur. Cette technologie était la seule, à cette époque, capable d'obtenir le degré d'intégration et la vitesse de fonctionnement nécessaires pour réaliser les circuits de cryptologie voulus et dont la consommation électrique était compatible avec les contraintes d'un matériel portable. Les circuits en MOS dynamique doivent toujours être cadencés par une horloge, sans quoi ils perdraient les informations qu'ils contiennent.

[24] Allusion au franc lourd de l'époque.

Des versions auto-synchronisantes, permettant de s'affranchir de la prise de synchronisation initiale et donc autorisant l'introduction immédiate d'un nouveau correspondant dans une communication déjà établie, ont aussi été étudiées et appliquées à certains types de réseaux.

C'est la clé de la CNT qui a servi de base au système de chiffrement du réseau RITA.

b) Une machine de chiffrement hors ligne a été réalisée spécialement pour la gendarmerie.

c) La famille FÉTICHE (Famille d'Équipements en Technologie Intégrée de Chiffre) dont les représentants les plus marquants sont le module FÉTICHE de chiffrement des artères du réseau RITA, et FETIDOC équipement de chiffrement des données jusqu'à 2 Mbits/s. Ces circuits sont dérivés de la CNT dont ils reprennent la logique. Mais avec FÉTICHE, un saut technologique est franchi en passant du MOS dynamique au circuit intégré en technologie TTL [25]. En effet, cette technologie offrait enfin un degré d'intégration compatible avec les besoins de la cryptologie tout en offrant des vitesses de fonctionnement très élevées.

d) L'appareil de discrétion téléphonique TRC 760 ; c'est un système de chiffrement analogique à découpage de bande conçu pour le camouflage des communications radio des forces du maintien de l'ordre (apparu souhaitable après les événements de mai 1968). Il fonctionnait en alternat. Une variante fonctionnant en duplex fut aussi développée : le TRC 765, qui est un système de chiffrement numérique et qui sera mis à la disposition de nos ministres, en 1977, dans sa version de bureau. Enfin, une version civile est également développée : le TRC 768.

e) La logique CRYPTOMOD (CRYPTOlogie MODulaire) incorporée dans le MAC (Mini Assemblage Crypto) permettant d'inclure la fonction chiffre dans les terminaux.

---

[25] Cette technologie est *a priori* plus rapide que la technologie MOS, mais sa capacité d'intégration est moindre.

f) Les systèmes de chiffrement pour les satellites : SAMRO, SPOT, TELECOM... Il s'agissait de protéger en intégrité les télécommandes (informations montantes, émises par les stations au sol) et en confidentialité les télémesures (informations descendantes émises par le satellite vers le sol). C'est pour ces applications que furent développés des algorithmes de chiffrement par blocs (16 et 32 bits), afin de satisfaire les hauts débits exigés par la liaison satellite.

g) La mise au point d'algorithmes de chiffrement par blocs de 64 bits pour des liaisons à haut débit (plus de 25 mégabits/s).

h) Le système de génération de fréquences pour les postes fonctionnant en évasion de fréquence (EVF) ou en étalement de spectre.

i) La cryptophonie haute sécurité (CHS) utilisant un vocodeur, d'abord à formant puis à prédiction linéaire. Ces travaux ont fait suite aux premières applications de Myosotis à la téléphonie de haute sécurité (cf. annexe II, paragraphe 4.3). C'est ainsi que SEIGNOL développa le système CYPHON. Ces travaux étaient accompagnés de nombreuses études sur l'analyse de la parole, études que menaient Jean-Pierre VASSEUR et Pierre DEMAN à Gennevilliers. Ces recherches étaient fortement soutenues par le STCCh qui avait le souci de protéger les communications téléphoniques des autorités étatiques. Malheureusement, ces mêmes autorités n'étaient absolument pas sensibles à cet aspect de la sécurité et il était très difficile de financer ces recherches.

j) La mise en œuvre et la conception de systèmes à « clé publique », dérivés du RSA (cf. le paragraphe 8 de l'annexe I). On cherchait à réduire les inconvénients du RSA (lenteur des opérations et taille des blocs d'information) en utilisant d'autres structures algébriques que les entiers modulo. Ces travaux ont été l'occasion d'une collaboration fructueuse avec l'Institut pour la Recherche en Informatique et Automatique (IRIA), principalement l'équipe de Jean VUILLEMIN, Philippe FLAGEOLET, Jacques VÉLU et Paul CAMION. De nouveaux dispositifs de distribution de clés en ont résulté.

k) Des études théoriques sur les problèmes nouveaux posés par l'évolution des machines à chiffrer (chiffrement par blocs, synchronisation...) et des techniques de décryptement en utilisant les résultats les plus récents de la théorie des automates, des demi-groupes ou des algorithmes (théorie de KROHN et RHODES, machines d'EILENBERG, etc.), et des propriétés algébriques et statistiques des fonctions booléennes.

La qualité des travaux réalisés et l'efficacité des équipes sont si bien reconnues par les responsables étatiques qu'en 1988, la Direction de l'électronique et de l'informatique, confie au laboratoire « Chiffre » de Thomson-CSF les études de base du « Chiffre gouvernemental », au terme d'une convention pluriannuelle. Il faudra attendre fin 1998, début 1999, pour que l'État, par l'intermédiaire du CASSI, organisme du Centre Électronique de l'Armement (CELAR), à Rennes, se dote d'une équipe de cryptologues, largement formés d'ailleurs au sein du laboratoire « Chiffre » de la Thomson-CSF.

Toutes ces réalisations ont bénéficié des progrès considérables de la micro-électronique (on gagne un facteur 2 tous les dix-huit mois, conformément à la loi de Moore). Cette miniaturisation a conduit naturellement à l'intégration complète de la fonction de chiffrement d'abord dans les terminaux puis dans les systèmes à protéger. Cette intégration s'accompagnait d'une automatisation de plus en grande des fonctions de chiffrement : le chiffre pouvait être mis directement dans les mains des utilisateurs sans passer par des chiffreurs, spécialistes de la mise en œuvre du chiffre.

Cette exploitation directe par les utilisateurs a impliqué une protection accrue des clés et a entraîné la mise au point de mécanismes de gestion automatique de ces clés. C'est pourquoi, aujourd'hui, lorsque l'on définit un nouveau système ayant des exigences de sécurité et de protection de l'information, il est nécessaire de prendre en compte cette fonction « sécurité » dès la conception du système pour que cette fonction soit sûre et aussi « transparente » que possible pour les utilisateurs.

Alors que le Chiffre devient une composante de plus en plus importante de nos systèmes d'armes, cette évolution est

caractérisée par une réduction progressive du rôle des chiffreurs et des services du Chiffre, ce qui ne les laissait pas sans inquiétude sur le devenir du Chiffre. Cependant l'introduction généralisée de l'informatique allait rapidement poser un problème encore plus vaste et plus complexe : celui de la protection des ordinateurs, si sensibles aux attaques et intrusions de toutes sortes.

Cette préoccupation touchait d'ailleurs tout le secteur civil, ainsi que nous l'exposons au paragraphe suivant. Désormais le problème majeur était celui de la Sécurité des Systèmes d'Information (SSI) dont le Chiffre n'était plus qu'une composante. Dès lors les chiffreurs devaient considérer leur métier comme une spécialité de la SSI.

IV.5. – L'ÉVOLUTION VERS LE CHIFFRE CIVIL NON GOUVERNEMENTAL.

Jusqu'alors, les activités « Chiffre » de la Thomson-CSF étaient strictement limitées aux applications gouvernementales : Chiffre étatique ou destiné à des organismes para-étatiques, sous le contrôle de l'État. Cela était d'ailleurs conforme à la législation concernant le contrôle gouvernemental sur l'utilisation des moyens de chiffrement. Or il était difficile pour la Thomson-CSF de maintenir une équipe importante compte tenu de l'étroitesse du marché gouvernemental, d'autant que les administrations françaises étaient très réticentes à lui donner un monopole de fait, alors qu'il n'y avait pas matière à faire vivre des équipes concurrentes.

Cependant, avec le développement de l'informatique et des télécommunications, les organismes civils ou privés, et surtout les banques, ont commencé à ressentir le besoin de protéger leurs informations. Il faut dire que les publications du DES (cf. le paragraphe 5 de l'annexe I) et des systèmes à clé publique (cf. le paragraphe 7 de l'annexe I) intriguaient beaucoup les « profanes » et ont créé une incontestable mode autour de la cryptologie.

En outre, sont apparues les premières chaînes de télévision à péage comme Canal Plus, que l'on baptisait chaînes « cryptées » car le signal d'émission était brouillé à l'aide d'un

algorithme de chiffrement. D'autre part, le développement des télécommunications civiles par satellites soulevait le problème de la discrétion de ces transmissions. Tout ceci a engendré un certain engouement pour la cryptographie dans le grand public et les entreprises privées.

De même, beaucoup d'universitaires mathématiciens se sont jetés sur ce nouveau domaine d'étude qui offrait des applications très concrètes et nouvelles à un sujet très abstrait et souvent difficile, quoique relativement élémentaire et ancien : la théorie des nombres.

Alors que cette matière était restée confinée au milieu des spécialistes de la cryptographie, une abondante littérature s'est développée dans pratiquement toutes les revues scientifiques, techniques ou industrielles. Mais, en général, elle a donné une vision rarement compréhensible, plutôt erronée et même contradictoire de la cryptographie. (Les méthodes de « cryptage » sont basées sur de grands nombres premiers ! Tous les systèmes de « cryptage » sont « cassés » ou « cassables ». Le système RSA est « inviolable »...) Cette vision, hélas, est encore largement répandue et on confond fréquemment sécurité des algorithmes, longueur des clés, secret parfait, secret pratique, etc. Des éclaircissements sont donnés à ce sujet au paragraphe 9 de l'annexe I.

Cette tendance s'est encore accentuée avec la création de nombreux congrès traitant de la sécurité de l'information, spécialisés ou non en cryptographie, sans compter maintenant les nombreux sites et forums de discussion sur Internet. Il en a résulté, dans le secteur civil, une grande confusion voire une incompréhension de ce qu'est le Chiffre et des conditions de son emploi.

Pressentant ce type de situation, la Thomson-CSF a essayé dès la fin des années soixante-dix d'orienter son activité « Chiffre » vers le secteur civil pour se positionner en tant que fournisseur de systèmes de chiffrement non gouvernementaux. Ainsi le laboratoire « Chiffre », sous l'impulsion de Joël LEBIDOIS, aidé par Pierre BÉNAITEAU, a lancé des études prospectives, élaboré des plans d'action et établi des contacts avec diverses grandes entreprises, en particulier, des banques.

C'est l'époque où celles-ci commençaient à se doter de systèmes de transferts de fonds électroniques, comme le réseau SWIFT *(Society for Worldwide Interbank Finantial Telecommunications),* systèmes très sensibles aux attaques et exigeant des mécanismes de haute sécurité.

L'idée de Joël LEBIDOIS était d'introduire les mécanismes cryptographiques dans les grandes applications du traitement de l'information, mais après avoir défini précisément les informations qui sont à protéger, et les attaques dangereuses qui sont susceptibles d'être montées. Il devenait alors possible de concevoir des mécanismes de protection adaptés aux utilisateurs de ces applications. Pour répondre à des besoins d'authentification, des dispositifs de sécurité spécifiques, comme des cartes (magnétiques ou à puces) d'authentification ou des systèmes biométriques (empreintes digitales, signature manuscrite, empreinte vocale), ont été étudiés, ainsi que leur intégration dans les terminaux.

De son côté, dès 1974 et avec le soutien de la DRET, Jean-Pierre VASSEUR avait lancé, avec Gilles RUGGIU, des études pour la protection des fichiers amovibles (suite au célèbre vol des fichiers sur bandes magnétiques de l'**O**ffice de **R**adiodiffusion-**T**élévision **F**rançaise) et des ordinateurs, en particulier des ordinateurs « multi-utilisateurs ».

L'idée de Jean-Pierre VASSEUR était d'adapter la structure des ordinateurs aux fonctions cryptographiques pour les intégrer au sein même de l'unité centrale. En effet, les détournements d'informations confidentielles sont tellement aisés dans un ordinateur, que les opérations de chiffrement doivent être réalisées au niveau du processeur si l'on veut garantir une haute sécurité afin que les informations confidentielles apparaissent en clair le moins souvent possible. De plus, lorsqu'elles sont en clair elles doivent rester confinées dans une enceinte protégée (il est malheureusement indispensable que ces informations soient en clair dans l'unité de traitement car les opérations de calcul et le chiffrement ne commutent pas !).

En outre, l'ordinateur doit travailler dans un environnement d'informations « multi-niveaux » : au moins deux niveaux de

classification doivent être gérés : le niveau confidentiel et le niveau non confidentiel puisque le processeur doit pouvoir traiter simultanément des informations confidentielles et des informations non confidentielles (les informations chiffrées doivent alors être déchiffrées pour restituer le clair au moment de leur traitement).

La gestion des clés dans une unité centrale pose des problèmes très complexes, car tout en étant automatique, cette gestion doit garantir la confidentialité, l'authenticité et l'intégrité des clés, sans dégrader les performances de l'ordinateur. Jean-Pierre VASSEUR et Gilles RUGGIU entreprirent alors une réflexion approfondie sur la sécurisation des ordinateurs, en prenant comme modèle de base la machine Edelweiss [26], ordinateur multiprocesseur « orienté langage » qu'ils étudiaient par ailleurs dans le cadre des recherches en informatique théorique qu'ils menaient en collaboration avec les universités Paris-VI et Paris-VII (à Jussieu).

Un comité de travail au niveau du groupe Thomson (regroupant DTC, LCR, CIMSA, LMT, TITN, le tout sous la tutelle de la direction technique générale) fut constitué en 1979 pour faire un état des lieux et lancer les actions prioritaires.

On constata que pour évoluer vers ces nouvelles conditions d'utilisation du chiffre, le champ d'action des équipes devait être élargi et bientôt l'axe majeur de ces activités devint la sécurité des systèmes d'information. Cependant, la difficulté majeure était de convaincre les utilisateurs de la validité de la solution proposée et de la capacité de résistance aux attaques des systèmes de sécurité offerts par cette solution, compte tenu de son coût. Mais, dans cette spécialité, d'un côté, les arguments que peut avancer un constructeur sont fragilisés par la valeur assez relative des preuves de sécurité, en particulier, pour les algorithmes cryptographiques ; d'un autre côté, les utilisateurs,

---

[26] J. ARSAC, C. GALTIER, G. RUGGIU, TRAN VAN KHAI, J.-P. VASSEUR, « The Edelweiss System », dans *Advances in Electronics and Electron Physics*, vol. 48, pp. 201-270, Academic Press (1979). Le langage de base de la machine Edelweiss était Exel, généralisation des langages Algol, Pascal et APL.

victimes de préjugés entretenus par la fâcheuse littérature concernant ce sujet, ne peuvent ou ne veulent entrer dans l'analyse de ces arguments. En dernier ressort, ce qui compte, c'est la confiance que les utilisateurs ont dans leurs fournisseurs.

Apparut alors l'idée de critères universellement reconnus et qu'un système ou un produit serait censé satisfaire. Ce nouveau domaine devait se concrétiser, au niveau international, par l'élaboration de critères d'évaluation de la sécurité des systèmes d'information. Il y eut d'abord la publication des critères TCSEC *(Trusted Computer System Evaluation Criteria)* du *Department of Defense* des États-Unis (DoD) en 1984. Ces critères avaient été bâtis à la suite de travaux théoriques portant sur la sécurité des ordinateurs que l'armée de l'Air américaine avait commandés, dès 1973, à la société *Mitre Corporation.*

Puis, les TCSEC furent suivis, en 1991, des critères ITSEC *(Information Technology Security European Criteria)* définis par la communauté européenne, mais en fait élaborés par quatre pays : la France, la Grande-Bretagne, l'Allemagne et la Hollande. C'est sur l'initiative des services du Chiffre de ces quatre États (devenus des services de la sécurité des systèmes d'information) et avec l'appui du SOGIS *(Senior Official Group for Information Security)* de la Commission de Bruxelles que furent créés ces fameux critères pour faire pièce aux critères américains TCSEC, lesquels étaient en fait pilotés par la NSA.

Ces critères ITSEC étaient le résultat de la fusion des critères nationaux dont ces quatre pays s'étaient dotés à la suite de la publication des TCSEC américains. D'autres critères internationaux virent le jour. Tous ces critères ont finalement convergé en 1995 avec l'établissement des Critères Communs, les « CC ». Ceux-ci, dans leur version 2.1, sont devenus une norme ISO internationale en août 1999 (norme ISO/IEC 15408, ISO signifie *International Organisation for Standard* et IEC, *International Electrotechnical Commission*).

Mais les obstacles étaient nombreux, non seulement parce que le laboratoire « Chiffre » de la Thomson-CSF était mal adapté pour répondre à ce type de demande, mais aussi en raison du contrôle gouvernemental qui s'exerçait de la même

manière qu'auparavant et que les entreprises du secteur civil comprenaient mal. Celles-ci s'accommodaient mal de la lenteur et de la parcimonie des décisions d'autorisation.

D'ailleurs le gouvernement français ressentit lui aussi la nécessité d'évoluer : le STCCh, qui, en 1976, était devenu, sous la direction d'André CATTIEUW, le Service Central des Chiffres et de la Sécurité des Télécommunications (SCCST), devint en 1986, à la demande de son chef de service et à la suite de plusieurs audits interministériels, le Service Central de la Sécurité des Systèmes d'Information (SCSSI). Ce nouveau service était placé sous l'autorité de la Délégation interministérielle pour la sécurité des systèmes d'information, créée à cette occasion, ce qui marquait l'extension des prérogatives de la cryptologie au domaine de la sécurité informatique, extension rendue nécessaire eu égard à l'émergence de la société informatisée.

En fait, ce ne fut que le début de nouvelles péripéties qui, avec la profusion des applications de l'informatique et des télécommunications, se poursuivent encore actuellement. Mais tous ces développements sortent du cadre de cet historique.

Cette évolution aurait pu être anticipée et donc mieux maîtrisée par la Thomson-CSF, si celle-ci avait su saisir l'occasion qui s'était présentée quelques années auparavant. En effet, Boris HAGELIN cherchait à vendre sa société CRYPTO-AG, installée en Suisse à Zug. Il avait pris contact, par l'intermédiaire d'André MULLER, avec la Thomson-CSF. Par la position particulière de CRYPTO-AG et de son marché, une telle acquisition aurait grandement renforcé le potentiel technique et commercial de la Thomson-CSF dans le domaine du chiffre civil non gouvernemental.

MULLER poussait beaucoup en faveur de cette solution. En effet, outre le renforcement de l'industrie française du Chiffre, il voyait dans cette reprise beaucoup d'avantages pour l'État français : HAGELIN vendait ses machines dans le monde entier et était une importante source de renseignements dont aurait bénéficié l'État français. Une première rencontre eut lieu, autour d'un déjeuner, entre Jean-Pierre VASSEUR, André MULLER et

Jean-Pierre BOUYSSONIE, le président de Thomson-CSF. Puis MULLER organisa une deuxième rencontre entre ce dernier et HAGELIN, en compagnie de CATTIEUW et RABAUD. Cette réunion eut lieu à Zug. Mais BOUYSSONIE ne se montra pas intéressé et l'affaire capota [27]. Finalement CRYPTO-AG fut rachetée par Siemens. Ce fut là, sans doute, une occasion manquée pour la Thomson-CSF.

[27] Mais il est très probable que les États-Unis, qui connaissaient bien CRYPTO-AG, n'auraient pas laissé se réaliser cette acquisition, étant donné le marché international (plus de 130 pays) que détenait cette société.

CONCLUSION

Le projet Myosotis fut la conséquence de la volonté de l'État français de se doter de moyens de chiffrement modernes, sûrs et adaptés à ses besoins. L'importance et la qualité des travaux qui ont abouti à la réalisation de cette machine ont permis de doter la France non seulement d'une doctrine du Chiffre cohérente, mais aussi de structures étatiques et industrielles qui l'ont placée au tout premier rang dans le monde dans le domaine de la cryptographie.

La position de la France s'est ensuite maintenue pendant une trentaine d'années grâce aux développements ultérieurs de nouveaux systèmes cryptographiques, développements dont la vigueur a encore été accentuée par les progrès considérables que l'électronique et les communications ont connus durant cette période. Avec l'introduction progressive de l'informatique dans les divers systèmes d'information, les conditions d'utilisation du Chiffre se sont considérablement modifiées en évoluant vers une intégration dans ces systèmes toujours plus poussée et une automatisation sans cesse accrue.

À partir du début des années quatre-vingt-dix, l'apparition du Chiffre civil et le formidable essor d'Internet ont posé de nouveaux problèmes. Les besoins des civils ainsi que leur façon d'utiliser le Chiffre étaient différents de ceux des gouvernements. De nombreux systèmes de chiffrement, en majorité d'origine américaine, sont alors apparus sur le marché dans une anarchie d'autant plus complète que les nouveaux utilisateurs du secteur civil n'avaient aucune compétence et aucun repère pour se faire une idée de leur valeur.

Les États, qui, comme la France, avaient une politique concernant l'emploi de moyens de cryptologie, avaient besoin de conserver un certain contrôle sur la fabrication et l'utilisation de ces moyens. Ils ont eu beaucoup de mal à réagir pour faire face à cette situation nouvelle d'autant plus que, comme pour tous les systèmes d'armes modernes, les outils développés dans ce domaine pour le civil ont un impact sur le militaire.

Un certain nombre de dispositions ont alors été prises, mais certaines erreurs ont été commises. Aujourd'hui encore, la situation du Chiffre en France, comme dans d'autres pays développés, est confuse et peu satisfaisante, instaurant, à l'opposé du but recherché, un climat de défiance envers la cryptographie et les services étatiques. Nous pouvons donc dire que, lorsque s'est effacée, au début des années quatre-vingt-dix, l'impulsion donnée par le projet Myosotis, une page de l'histoire de la cryptographie en France a été tournée.

ANNEXE I

LES PRINCIPES DE LA CRYPTOGRAPHIE

1. – Définitions

Le mot cryptographie provient des deux mots grecs :

– *kruptos*, qui veut dire secret (ou caché, dissimulé),
et
– *graphein*, qui veut dire écrire.

En accord avec cette étymologie, on définit la cryptographie comme la science (ou l'art) des écritures secrètes [28].

Par « écritures secrètes », il faut entendre les modifications que l'on fait subir à un texte ou à un message en vue de le rendre incompréhensible à ceux qui n'ont pas à le connaître. Ces modifications constituent une transformation qui caractérise la méthode de chiffrement. Pour retrouver le texte initial, il faut connaître la transformation inverse de la précédente. Celle-ci doit donc rester secrète et connue des seuls correspondants qui désirent échanger des messages confidentiels.

Le texte initial est appelé « clair », le résultat de la transformation est le cryptogramme ou « crypto » en abrégé. L'élaboration du crypto à partir du clair s'appelle un **chiffrement** : on dit que l'on chiffre le message ; l'opération inverse est un **déchiffrement** : on déchiffre le message.

2. – Exemples et principes des systèmes de chiffrement.

On sait que depuis la plus haute Antiquité, les hommes se sont dotés, à côté de leurs systèmes d'écriture normaux, c'est-à-dire connus de tous, d'autres systèmes d'écriture connus des seuls initiés. Parmi les systèmes secrets qui nous sont rapportés par l'histoire, on peut en citer deux qui sont remarquables.

---

[28] A. MULLER, *Les Écritures secrètes*, Paris, PUF, Collection Que sais-je ?, 1971 ; *Le Décryptement*, Paris, PUF, Collection Que sais-je ?, 1983.

Ainsi PLUTARQUE raconte qu'au Vᵉ siècle avant J.-C., à Sparte, les messages échangés avec les armées en campagne étaient chiffrés au moyen d'un ingénieux instrument : la scytale. Celle-ci se présentait comme un bâton de forme cylindrique. Par une fente située à une extrémité du bâton, on introduisait une lanière qu'on enroulait en spires jointives. On écrivait le texte dans le sens de la longueur du bâton (c'est-à-dire le long des génératrices). La lanière une fois déroulée portait les mêmes lettres que le texte initial mais dans un ordre différent. À la réception, il suffisait d'enrouler la lanière autour d'un bâton de même diamètre pour pouvoir lire le message. Une telle transformation s'appelle une **transposition,** car si toutes les lettres du texte clair sont conservées, elles ne sont plus dans le même ordre.

L'autre exemple nous est donné par Jules CÉSAR. Pendant la guerre des Gaules, celui-ci avait l'habitude de modifier ses textes de différentes manières. Il remplaçait, par exemple, les lettres latines par des lettres grecques (le texte restant en latin) ; ou bien il remplaçait la lettre « a » par la lettre « d », la lettre « b » par « e », « c » par « f », et ainsi de suite, c'est-à-dire qu'il décalait l'alphabet normal de trois lettres. Ce type de transformation s'appelle une **substitution** : chaque lettre est remplacée par une autre, toujours la même.

La transposition et la substitution sont les transformations de base de la cryptographie. Réciproquement, tout système de chiffrement est toujours équivalent à une suite de ces deux types de transformations.

3. – La notion de clé secrète.

En pratique, il est difficile de conserver secrète une méthode de chiffrement, compte tenu du fait qu'il faut distribuer aux utilisateurs (les chiffreurs) les matériels nécessaires, qu'il faut les former et stipuler les conditions de sa mise en œuvre.

Pour simplifier le travail des chiffreurs, on fait dépendre la méthode de chiffrement d'une information auxiliaire qu'on

appelle la **clé.** Par exemple pour le second chiffre de Jules CÉSAR, la clé est le décalage entre les deux alphabets, qui ici vaut 3. Dans le cas de la scytale, on peut considérer que la clé est le diamètre du bâton, bien que cette clé soit assez facile à deviner (la scytale doit plutôt être considérée comme un système sans clé).

Si le système de chiffrement est bien conçu toute la sécurité repose non pas sur le secret de la méthode, mais sur le seul secret de la clé. La méthode peut donc être diffusée sans précaution particulière.

C'est l'Italien BELASO qui, en 1553, a eu l'idée d'introduire cette notion de clé secrète et la façon de l'utiliser. La clé doit être simple à utiliser, sinon c'est le système de chiffrement qui devient inutilisable, mais elle ne doit pas être simple à deviner par un éventuel attaquant.

Tous les systèmes de chiffrement modernes reposent sur ce principe. Précisons que les clés de chiffrement et de déchiffrement ne sont pas nécessairement identiques. Cela dépend de la méthode de chiffrement. Lorsque ces deux clés sont identiques ou que l'une est facilement déductible de l'autre, alors toutes deux doivent rester secrètes. Ces systèmes sont dits **symétriques.**

En pratique, quand un grand nombre d'utilisateurs d'un système de chiffrement doivent communiquer entre eux, ils peuvent être amenés à utiliser un grand nombre de clés qui deviennent difficiles à gérer. En fait, dans un réseau de communication, le chiffrement peut être réalisé soit au niveau des postes émetteurs ou récepteurs (chiffrement de bout en bout), soit au niveau des liaisons (chiffrement d'artères). Le chiffrement d'artères simplifie la gestion des clés. Cette gestion se simplifie aussi quand les utilisateurs sont organisés en sous-réseaux et que les membres d'un même sous-réseau partagent la même clé.

Si, au contraire, il est **matériellement** impossible de calculer la clé de déchiffrement à partir de celle de chiffrement, alors on conçoit qu'il soit possible de faire connaître la clé

de chiffrement (on dit qu'elle est publique) sans compromettre le secret du déchiffrement. Ces systèmes sont dits **asymétriques** [29].

Notons qu'un système symétrique garantit au destinataire l'authenticité de l'émetteur, puisque celui-ci est le seul (avec le destinataire) à posséder la clé de chiffrement, alors qu'un système asymétrique n'a pas cette propriété, car la clé de chiffrement (publique) est connue de tous.

Les systèmes asymétriques réalisent donc une **disjonction** des fonctions de **confidentialité** et d'**authentification.** Mais, en raison même de cette disjonction, ils sont sensibles aux risques d'intrusion, car tout individu a accès à la clé publique (le destinataire n'a donc aucune garantie de l'identité de l'émetteur). La clé publique peut, elle-même, être falsifiée et dans ce cas l'émetteur n'a aucune garantie de l'identité du destinataire ; et en cas d'utilisation d'une clé falsifiée par un espion, non seulement l'espion est en mesure de déchiffrer le message, mais le destinataire authentique est dans l'incapacité de le faire.

Il est donc nécessaire de compléter ces systèmes asymétriques par des mécanismes d'authentification spécifiques. Ces mécanismes peuvent être réalisés soit avec des systèmes cryptographiques symétriques, à l'aide de **tiers de confiance** jouant le rôle de notaires (électroniques) chargés de gérer les clés secrètes, soit avec des systèmes asymétriques où les rôles de la clé publique et de la clé secrète sont inversés (la clé secrète garantit l'identité de son détenteur). Ce sont ces mécanismes qui sont à l'origine de la **signature électronique.** Nous revenons sur ce sujet au paragraphe 8.

---

[29] Précisons qu'un constructeur de système à clé publique doit être en mesure de calculer simultanément la clé secrète et la clé publique grâce à une information qu'il doit garder secrète, information appelée « chausse-trappe ». Un attaquant qui ne connaît pas cette chausse-trappe ne peut à partir de la seule clé publique reconstituer la clé secrète. C'est cette condition qui rend très difficile la mise au point d'un système à clé publique et qui explique qu'il y en a peu.

4. – **La notion de décryptement.**

En réalité, la définition étymologique que nous venons de donner est incomplète. La cryptographie comporte un second aspect que les spécialistes appellent **« analyse cryptographique », « décryptement » ou « cryptanalyse ».**

Autrement dit, et en accord avec la définition du commandant BAUDOUIN [30], la cryptographie ne se limite pas à l'étude des procédés de chiffrement, mais elle cherche aussi les méthodes permettant de les décrypter.

Si le but du chiffre est de rendre un clair incompréhensible pour ceux qui n'en possèdent pas la clé, le décryptement a pour objet le rétablissement du clair sans connaître la clé nécessaire pour le déchiffrement. Une bonne conception d'un système de chiffrement, doit rendre le décryptement très difficile, l'idéal étant qu'il soit impossible. Lors de la conception d'une machine à chiffrer, on effectue en parallèle sa cryptanalyse, afin de s'assurer qu'il est impossible (matériellement) de la décrypter. C'est l'objectif essentiel de son **évaluation,** l'autre objectif de l'évaluation étant de tester les conditions de sa mise en œuvre et de son exploitation.

Il faut bien comprendre que le décryptement pose en fait **deux problèmes** liés mais distincts. Le premier consiste à retrouver le clair à partir du crypto (qui, par hypothèse, a été intercepté) ; c'est ce qu'on appelle décrypter le message. Le second consiste à déterminer, à partir d'un ou plusieurs cryptos interceptés, la clé qui a été effectivement utilisée. En principe la solution du second problème entraîne celle du premier, puisque dès que l'on est en possession de la clé, on est capable de déchiffrer le message comme le véritable destinataire. Mais la réciproque n'est pas vraie : ce n'est pas parce que l'on a pu retrouver le clair d'un crypto que l'on sait déterminer la clé. La différence est importante, car lorsque l'intercepteur a rétabli la clé, il est alors en mesure de déchiffrer tout autre

---

[30] Roger BAUDOUIN, *Éléments de cryptographie,* Paris, éditions Pédone, 1939, 1re édition.

message qui a été chiffré avec la même clé (il n'a plus besoin de le décrypter).

Lorsque, pour un système de chiffrement, on est en possession d'une méthode générale de décryptement, c'est-à-dire d'une méthode indépendante du message clair à décrypter et de la clé utilisée, on dit que l'on a décrypté ou « cassé » ce chiffre. Bien entendu dès lors que l'on sait qu'un chiffre a été cassé, celui-ci ne doit plus être utilisé. C'est pourquoi d'ailleurs, un service ou un individu qui a cassé un chiffre s'en vante rarement, sans quoi il perd tout le bénéfice de son travail [31] !

En pratique, pour évaluer un système de chiffrement, on étudie aussi les possibilités de **décrypter partiellement** des messages. On analyse par exemple les conditions dans lesquelles on peut retrouver des parties (quelques bits, voire un seul bit) d'un message clair à partir de son crypto ; ou encore, étant donné deux cryptos et deux clairs, on vérifie que l'on n'a pas plus d'une chance sur deux d'attribuer le bon crypto à chaque clair.

5. – Les premières machines à chiffrer.

Autrefois les opérations de chiffrement se faisaient manuellement. Mais dès le XV^e^ siècle, le grand architecte florentin Léon ALBERTI inventa un cryptographe : c'était un appareil permettant d'effectuer mécaniquement des substitutions. Les appareils de ce type sont pratiquement restés inchangés jusqu'au début du XX^e^ siècle.

C'est durant la Première Guerre mondiale qu'apparaissent les premières machines à chiffrer mécaniques ou électriques. Ainsi en 1917, l'Américain Gilbert VERNAM, de la compagnie AT&T, invente le téléimprimeur chiffrant, basé sur le code Baudot et utilisant comme clé une bande perforée contenant une suite de caractères aléatoires. Cette bande devait être changée à chaque chiffrement, c'est pourquoi ce système était appelé **« bande clé une fois ».**

---

[31] Comme le dit John LAFFIN : « Un véritable expert en cryptographie ne se vantera jamais de sa science », dans *Petit code des codes secrets,* Paris, éditions Arts et Voyages, 1968, p. 22.

L'année suivante, l'ingénieur allemand Arthur SCHERBIUS déposait le brevet de la fameuse machine Enigma qui fut adoptée par les Allemands lors de la Seconde Guerre mondiale. Parmi les constructeurs européens importants à cette époque, on peut citer Hagelin (Suède) qui installa sa société CRYPTO-AG en Suisse, Siemens (Allemagne) et Olivetti (Italie).

En général, les machines à chiffrer réalisent uniquement des procédés de substitution car la transposition, qui exige la mémorisation de longues portions de messages, n'est pas simple à automatiser (elle augmenterait considérablement le délai de transmission des messages).

Les substitutions réalisées par les machines à chiffrer portent sur un petit nombre de bits et représentent pratiquement toujours un caractère : 5 bits pour le code Baudot à cinq moments, 7 bits ou 8 bits pour les codes ASCII. Quand le calcul du crypto s'effectue sur un seul bit, la substitution est une addition modulo 2, bit à bit (ou son complément). Ce mode de chiffrement est souvent appelé **« chiffrement par flot ».**

Actuellement, grâce à la grande puissance de calcul des processeurs (spécialisés ou non) on peut traiter beaucoup plus de bits en parallèle : on parle alors de **« chiffrement par blocs ».** Ainsi l'algorithme DES *(Data Encryption Standard),* dérivé du système IBM Lucifer, définit une substitution sur 8 lettres, soit des blocs de 64 bits. Le DES est né d'un appel public à contribution du bureau des standards américain (NBS) en mai 1973 pour la conception d'un algorithme de chiffrement destiné à protéger les informations (non classifiées de Défense). Il a été publié en 1975 et normalisé en 1977 par le NBS.

6. – La théorie des systèmes secrets.

C'est à la Renaissance que les premiers traités de cryptographie sont apparus (ALBERTI, TRITHÈME, VIGENÈRE, PORTA...) ainsi que les premières formulations en termes mathématiques (François VIÈTE). Le mathématicien et physicien Jérôme CARDAN invente en 1550 le principe de l'**autoclave.** Ce principe consiste à faire dépendre du clair la procédure de

calcul du crypto (le clair définit sa propre clé). C'est un procédé très efficace, mais qui a l'inconvénient d'augmenter les erreurs au déchiffrement en cas de mauvaise transmission. Au XVII[e] siècle, le chiffre connaît une période brillante avec Antoine ROSSIGNOL en France et le mathématicien John WALLIS en Angleterre.

Puis une période de déclin commence au milieu du XVIII[e] siècle qui a perduré jusque vers la fin du XIX[e] siècle. En 1863, l'Allemand Friedrich KASISKI publie un remarquable petit livre de cryptanalyse, mais malheureusement celui-ci passe inaperçu. Il donnait la solution du décryptement du système poly-alphabétique de VIGENÈRE, considéré pendant plus de trois siècles comme indécryptable. Il est permis de penser que ce décryptement a été réalisé beaucoup plus tôt, mais ses auteurs se sont bien gardés de le faire savoir.

Il faut attendre 1883 pour que la cryptographie retrouve son éclat avec l'ouvrage du français d'origine belge Auguste KERCKHOFFS, *La Cryptographie militaire,* qui est à l'origine du regain d'intérêt pour la cryptologie en France et à l'étranger. Il y donnait une approche moderne de la cryptographie. KERCKHOFFS est aussi l'inventeur d'un petit cryptographe manuel, mais très commode : la réglette de Saint-Cyr. En même temps se fondent les bases scientifiques de la cryptographie et de la cryptanalyse grâce au développement du calcul des probabilités, de la statistique et des structures algébriques modernes : algèbre de Boole, groupes, corps finis, théorie des automates...

Enfin, la cryptologie acquiert ses lettres de noblesse avec le travail fondamental de Claude SHANNON pendant la Seconde Guerre mondiale dans le laboratoire de la compagnie Bell Telephone, aux États-Unis. Ces résultats, restés un temps secrets, sont publiés en janvier 1949 [32]. Le point de départ de SHANNON est la notion d'information dont il donne une définition très générale : la réalisation d'un événement de probabilité p apporte l'information $I = -\log_2 p$ [33] : l'information est proportionnelle à l'inverse de la probabilité (un événement rare

[32] « Communication Theory of Secrecy Systems », *Bell System Technical Journal,* vol. 28, octobre 1949, pp. 656-715.

[33] Cette notation désigne le logarithme en base 2.

apporte beaucoup d'informations). Il définit alors l'entropie ou l'incertitude moyenne d'un ensemble d'événements « E » par la formule :

$$H = - \sum_i p_i \log_2 p_i,$$

où « i » parcourt les événements de « E ». Les messages sont considérés comme des événements émis par une source. Celle-ci code les messages à l'aide d'un alphabet et l'ensemble de tous les messages susceptibles d'être émis constitue le langage de la source. La **redondance** d'un langage provient de la différence entre ce langage et l'ensemble de tous les messages possibles, c'est-à-dire l'ensemble de toutes les suites de caractères que l'on peut écrire avec l'alphabet de la source. C'est d'ailleurs en étudiant les systèmes de chiffrement que SHANNON a élaboré sa théorie de l'information [34], qui généralise les travaux antérieurs, en particulier ceux de HARTLEY qui donna en 1928 une première définition quantitative de l'information.

SHANNON introduit la notion de **secret parfait** : un système de chiffrement est parfait lorsque les probabilités *a posteriori* des clairs sont toujours égales aux probabilités *a priori* correspondantes, quels que soient les cryptogrammes interceptés (c'est-à-dire que la capture d'un crypto ne peut apporter aucune information nouvelle susceptible d'aider au décryptement). Il montre alors qu'une condition nécessaire pour qu'un système soit parfait est que l'entropie des clés soit supérieure ou égale à celle des clairs : autrement dit, on doit utiliser autant de clés que de clairs et chaque clé doit être aussi longue que le clair. C'est le principe des **« clés une fois »** du système de Vernam.

Malheureusement ce type de système n'est utilisable que dans des conditions exceptionnelles. En pratique, les clés sont utilisées plusieurs fois et doivent être très courtes, comparées à la longueur du clair. Mais le système est alors potentiellement (ou théoriquement) décryptable et SHANNON montre que la longueur minimale de crypto nécessaire pour réussir un décryptement est égale à l'entropie des clés divisée par la redondance du langage. Cette longueur est appelée **distance d'unicité** du

[34] « A Mathematical Theory of Communication », *Bell System Technical Journal,* vol. 27, juillet 1948, p. 379 et octobre 1948, p. 623.

système de chiffrement. Comme la redondance est d'au moins 70 % pour la plupart des langues naturelles, la distance d'unicité est inférieure à une fois et demie la longueur des clés. C'est donc la redondance du langage source qui donne la possibilité de réussir un décryptement.

De la même façon, plusieurs messages chiffrés avec la même clé ouvrent la voie au décryptement : c'est ce que l'on appelle des **messages parallèles.** On montre que le nombre **dangereux** de messages parallèles est de l'ordre de la distance d'unicité divisée par la longueur des messages parallèles.

Mais, **en pratique,** le secret peut être aussi assuré si le travail nécessaire pour réussir le décryptement est tellement considérable qu'il est vain de l'entreprendre. SHANNON donne des indications pour évaluer ce travail. En tout état de cause, ce travail est, en moyenne, inférieur à $\alpha 2^{H(K)-1}$, où H(K) est l'entropie des clés et α le travail pour essayer une clé. En effet, on peut toujours les essayer toutes et on a une chance raisonnable de trouver la bonne clé après avoir essayé la moitié des clés possibles (c'est la méthode des **essais systématiques**). Ainsi un système de chiffrement utilisant des clés de 128 bits est inattaquable par les essais systématiques (il faudrait en faire environ $2^{127} \# 10^{38}$), et peut donc être considéré comme indécryptable, à condition, bien sûr, que l'algorithme soit bien conçu, c'est-à-dire qu'il n'existe pas d'autres méthodes de décryptement plus efficace.

7. – La complexité des algorithmes et le problème du décryptement.

C'est au milieu des années soixante-dix que l'on a pu mieux formaliser cette évaluation du travail de décryptement grâce au développement de la théorie de la complexité des algorithmes. Cette théorie répondait initialement aux besoins de la logique mathématique (pour mieux caractériser les fonctions calculables) et de l'informatique.

La complexité d'un algorithme se mesure généralement par le nombre d'étapes de calcul nécessaires pour obtenir le résultat.

Ce nombre « n » dépend de la longueur « l » des données et aussi des moyens de calcul utilisés. Mais la loi définissant la variation, en fonction de « l », de l'ordre de grandeur de « n » : O(n), est indépendante de ces moyens de calcul et ne dépend que de « l » : O(n) = f(l). Si « f » est une fonction puissance (du premier degré, du second degré...), on dit que l'algorithme est polynomial (linéaire, quadratique...) ; si « f » est une exponentielle (de la forme a^l), l'algorithme est exponentiel. Quand O(n) dépasse, disons, 10^{30}, on conçoit que l'algorithme correspondant soit infaisable en pratique : supposons que l'on dispose d'un milliard d'ordinateurs capables d'effectuer chacun mille milliards d'opérations par seconde, il faudrait tout de même attendre trente-deux ans pour obtenir le résultat (en supposant qu'une opération suffise pour effectuer une étape de calcul). Précisons qu'un même problème peut être résolu par des algorithmes ayant des complexités différentes. La complexité d'un problème (dont on connaît au moins un algorithme de résolution) est celle de l'algorithme de résolution ayant la plus faible complexité.

Le problème général du décryptement n'a pas d'algorithme de résolution puisqu'on connaît une classe de systèmes de chiffrement indécryptables : les systèmes à secrets parfaits. En revanche, les systèmes de chiffrement dont la longueur des clés est fixée, disons **m** bits, peuvent être décryptés en essayant toutes les clés possibles comme nous l'expliquons au paragraphe précédent (à condition de posséder un crypto dont la longueur dépasse la distance d'unicité du système, ce qui suppose que le langage source est redondant). Mais la complexité de cet algorithme est exponentielle puisque *a priori* il faut essayer $\mathbf{2^m}$ clés. Par conséquent, dès que m est assez grand (disons supérieur à 100) cet algorithme est impraticable. À l'heure actuelle, on ne sait pas s'il existe un algorithme général, c'est-à-dire applicable à tous les systèmes de chiffrement dont la longueur des clés est finie, meilleur que celui-ci, et on pense qu'il n'en existe pas.

8. – Les systèmes à clé publique.

L'étude de la complexité des algorithmes permettant de passer des clés de chiffrement aux clés de déchiffrement a ouvert la

voie des systèmes asymétriques, souvent appelés (improprement) systèmes à clé publique (voir le paragraphe 3 ci-dessus). Dans ces systèmes, l'asymétrie des clés est telle que la connaissance de l'une d'elle ne permet pas de calculer l'autre (dans un temps raisonnable). Il suffit alors de garder secrète la clé de déchiffrement, tandis que la clé de chiffrement peut être rendue publique (pour la signature, les rôles sont inversés : la clé de signature est gardée secrète et la clé de vérification de la signature peut être rendue publique).

Le système dit à « **double cadenas** » permet même de s'affranchir de toute distribution de clés. Le message est chiffré par son émetteur avec sa propre clé (il met son cadenas) ; le destinataire le surchiffre avec sa propre clé (il met un deuxième cadenas) et le renvoie à l'émetteur ; celui-ci le déchiffre avec sa clé (il reste le cadenas du destinataire) et le renvoie une deuxième fois ; le destinataire déchiffre le message avec sa clé (il enlève le second cadenas). Ce mécanisme multiplie le trafic par trois (un aller et retour suivi d'un envoi), mais aucun correspondant n'a eu à échanger des clés. Il suppose que les opérations de chiffrement sont commutatives entre elles puisque les déchiffrements n'ont pas lieu dans l'ordre inverse des chiffrements. Mais les opérations de chiffrement sont rarement commutatives !

On peut résumer la situation par le tableau suivant :

MÉTHODE de chiffrement	CONFIDENTIALITÉ de la transmission	AUTHENTIFICATION du destinataire	AUTHENTIFICATION de l'émetteur
Systèmes à clés secrètes	OUI	OUI	OUI
Systèmes à clé publique	OUI si la clé de chiffrement est authentique	OUI si la clé de chiffrement est authentique	NON
Systèmes à double cadenas	OUI	NON	NON

C'est dans le contexte du chiffre civil, où chacun peut vouloir correspondre confidentiellement avec n'importe qui sans disposer d'une organisation de gestion de clés, que les systèmes

à clés publiques trouvent leur intérêt. Mais se pose alors le problème de la **confiance** dans les clés utilisées. Et le tableau précédent montre que cette question est cruciale.

En général, les clés publiques sont accompagnées de **certificats** qui garantissent leur authenticité. Ces certificats, délivrés par des **autorités de certification** reconnues des utilisateurs, sont gérés au moyen d'un **annuaire** public. Pour qu'un tel système soit utilisable, il faut absolument garantir l'intégrité, l'authenticité et la disponibilité de l'annuaire, sans quoi toutes sortes d'intrusions et de falsifications deviennent possibles (comme indiqué au paragraphe 3 précédent). Les outils mettant en œuvre ces mécanismes sont appelés **Infrastructure de Gestion de Clés,** ou IGC (en terme anglo-saxon, *Public Key Infrastructure,* PKI). La confiance réside alors dans celle que les utilisateurs accordent à l'autorité de certification utilisée, qui joue le rôle de tiers de confiance. Cela rejoint le principe des systèmes à clés secrètes, mais avec une organisation allégée quand il y a beaucoup d'utilisateurs.

Le principe des systèmes à clé publique a été publié pour la première fois par DIFFIE et HELLMAN en 1976 et ils ont proposé en même temps deux protocoles : un, pour l'établissement de clés communes à deux utilisateurs d'un système de chiffrement, et un autre, pour la transmission de messages chiffrés sans échange de clé (méthode du double cadenas). Ces deux protocoles sont basés sur le calcul d'une exponentielle modulo un nombre premier.

Beaucoup de systèmes à clé publique ont été proposés mais pratiquement tous ont été cassés. Le seul qui tienne encore la route est aussi le premier qui ait été publié (en avril 1977) : le système RSA, du nom de ses inventeurs : RIVEST, SHAMIR et ADLEMAN. Il consiste à calculer une exponentielle modulo un nombre n, qui est lui-même le produit de deux facteurs premiers. On montre que la sécurité du système repose sur la difficulté de retrouver ces deux facteurs, connaissant « n », c'est-à-dire de factoriser ce nombre. Et dans l'état actuel de nos connaissances mathématiques et algorithmiques, la factorisation d'un nombre est un problème difficile.

Les systèmes à clé publique ne peuvent être utilisés qu'en mode de chiffrement par blocs de très grande taille. En effet, connaissant la clé publique, on peut attaquer le système en préparant à l'avance les cryptos de tous les clairs possibles. Soit « B » la taille des blocs ; le nombre de clairs est de l'ordre de $2^{B(1-\rho)}$, où ρ est la redondance du langage. Pour que la complexité de cette attaque soit équivalente à celle des essais systématiques d'un système de chiffrement à clés secrètes de, mettons 120 bits, la taille des blocs doit faire plus de 400 bits (en supposant une redondance de 70 %, ce qui est réaliste).

Autrement dit, tout système à clé publique, y compris RSA, dont les messages sont des blocs de taille inférieure à 400 bits doit être considéré comme étant cassable. Cela montre que les systèmes à clé publique ne sont pas utilisables manuellement, puisque le chiffrement de messages dont la longueur est d'au moins 400 bits n'est réalisable qu'avec des moyens informatiques. La longueur de ces blocs impose de nombreuses précautions quand les messages clairs sont courts. Ceux-ci doivent être judicieusement complétés pour atteindre la longueur voulue des blocs. Par exemple, le RSA laisse systématiquement passer un bit du clair : il ne chiffre pas le **symbole de Jacobi** [35]. En effet, on montre facilement que la valeur du symbole de Jacobi du cryptogramme est la même que celle du clair. Si donc, on utilise RSA pour chiffrer les deux messages « OUI » ou « NON », on doit recourir à un mécanisme de complétion capable de masquer aléatoirement le symbole de Jacobi de chacun d'eux, sinon le chiffrement est inefficace.

En réalité, les systèmes à clé publique, ont été découverts par l'Anglais James ELLIS du CESG (*Communications-Electronics Security Group,* équivalent britannique du STCCh) dès la fin des années 1960. James ELLIS a décrit le RSA en janvier 1970 dans une note interne au CESG. L'idée de départ de James ELLIS était que, s'il n'y a pas d'échange de secret entre l'émetteur et le récepteur, alors ce dernier, comme l'émetteur,

[35] Le symbole de Jacobi d'un nombre, appartenant à l'ensemble des nombres entiers modulo N, vaut 1 ou –1, avec la même probabilité. Il donne donc un bit d'information sur ce nombre.

doit participer à l'élaboration de la clé. Un collègue de ELLIS, Malcolm WILLIAMSON, devait découvrir, deux mois après la note de James ELLIS, les deux protocoles de DIFFIE et HELLMAN. Mais ces découvertes ont été soigneusement tenues secrètes et elles ne furent rendues publiques que trente ans plus tard, en 1998 [36].

Signalons qu'en France, au STCCh, J. FAVARD avait, dès 1960, proposé d'utiliser des exponentielles modulaires ou des logarithmes discrets comme fonctions de chiffrement, et il étudia les propriétés des alphabets chiffrants ainsi formés, mais pour des alphabets ordinaires, donc des lettres constituées d'un petit nombre de bits (5 bits). Cette idée venant trop tôt, il n'alla pas plus loin, sans doute à cause de l'impossibilité pratique d'effectuer ces calculs avec les moyens de l'époque [37].

9. – **Longueur des clés et sécurité des systèmes de chiffrement.**

La longueur des clés est un paramètre important du niveau de sécurité offert par un système de chiffrement, comme le montre la théorie de Shannon. Cependant, il est loin d'être l'élément caractéristique de cette sécurité, contrairement à une idée très largement répandue dans le public non averti. Ce qui a beaucoup contribué à populariser ce point de vue regrettable, c'est plusieurs décisions prises par divers gouvernements au cours des années quatre-vingt-dix. Ainsi les Américains ont autorisé l'exportation de systèmes de chiffrement dont la longueur des clés est inférieure à 40 bits ; le gouvernement français a libéré l'utilisation du chiffre si les clés ne dépassent pas 40 bits, seuil qui a été ensuite porté à 128 bits. Ceci laissa penser que tous les systèmes de chiffrement dont les clés font moins de 40 bits sont aisément cassables, du moins avec les

[36] Selon certaines rumeurs, la NSA aurait aussi découvert les systèmes à clé publique en 1961.

[37] Rappelons qu'à ce moment-là, le problème de la gestion d'un grand nombre de clés au sein d'un grand réseau ne se posait pas : les services du Chiffre disposaient d'une organisation rodée et efficace pour distribuer les clés. Il n'y avait donc aucun besoin d'imaginer de nouveaux systèmes de distribution de clés.

moyens dont peuvent disposer des services gouvernementaux, et ceux dont les clés dépassent 128 bits restent incassables [38].

La réalité est tout autre. On peut réaliser des systèmes de chiffrement dont les clés font plusieurs centaines de bits et qui sont parfaitement cassables. C'est par exemple le cas si les différents bits des clés sont mal utilisés ou si l'algorithme de calcul du crypto présente des faiblesses facilement exploitables, faiblesses souvent engendrées par une complexité illusoire. *A contrario,* un chiffre de 40 bits de clé peut être extrêmement robuste. Il suffit pour cela que chaque essai d'une clé nécessite un travail préparatoire assez long, disons de l'ordre d'une seconde (ce qui n'est pas incompatible avec une vitesse de chiffrement élevée, par exemple de plusieurs millions de bits par seconde). Il faudrait alors faire travailler simultanément pendant dix ans un million de machines à décrypter afin de réaliser les 2^{40} essais nécessaires à la réussite du décryptement ! Notons que ces machines seraient spécialisées pour ce système de chiffrement et il faudrait en faire autant pour tout autre système de chiffrement.

On a vu que les systèmes à clé publique exigent des clés d'au moins 400 bits. Le système offrant les meilleures garanties de sécurité, c'est-à-dire RSA, doit aujourd'hui utiliser des clés de 2 048 bits, longueur qu'il faudra sans doute doubler d'ici une vingtaine d'années [39]. C'est dire la fragilité de ces systèmes.

En fait, le niveau de sécurité d'une machine à chiffrer résulte de trois éléments :

- la longueur (ou l'entropie) des clés ;
- les principes de l'algorithme de calcul du crypto, de sa mise en œuvre et de l'utilisation des clés ;
- les conditions et l'environnement d'exploitation du système.

---

[38] Cf. l'article de J.-L. DESVIGNES, *Bulletin de l'ARCSI,* n° 30, 2002, pp. 27-40.

[39] La formule de Brent donne l'année Y où la factorisation d'un nombre de D chiffres décimaux sera possible : $Y = 13{,}24. (D^{1/3}) + 1928{,}6$. Pour des nombres de 2 048 bits on trouve 2 041. Mais cette formule ne tient pas compte des progrès des algorithmes de factorisation.

Il est nécessaire d'évaluer l'ensemble de tous ces éléments pour valider le niveau de sécurité du système de chiffrement, tout en sachant qu'il n'existe aucune preuve mathématique que celui-ci est « incassable » !

10. – **La stéganographie et la cryptographie quantique.**

La stéganographie est l'art de dissimuler les informations secrètes pour les rendre inaccessibles aux espions. Il s'agit donc de procédés physiques ou plutôt chimiques, comme les encres sympathiques ou invisibles ; ils sont le plus souvent d'une efficacité très limitée. Ils sont généralement utilisés en complément de la cryptographie classique.

Cependant une technique nouvelle a été proposée en 1982, d'après une idée originale conçue par S. WIESNER autour de 1970. La cryptographie quantique met à profit le principe d'incertitude d'Heisenberg, principe qui joue un rôle fondamental en mécanique quantique. *A priori* le niveau de sécurité qu'elle offre est donc comparable au niveau de certitude des prédictions de la mécanique quantique (qui, jusqu'à présent, se sont toujours avérées exactes, avec une très grande précision).

Le protocole mis en œuvre par la cryptographie quantique permet non seulement de dissimuler aux intrus les informations transmises mais de détecter d'éventuelles intrusions et de les éliminer. Il utilise deux canaux de transmission : un canal classique et un canal quantique.

Pour en expliquer le principe, supposons que l'objet physique transportant un bit d'information soit un photon et que la polarisation du photon serve à coder l'information. À l'émission deux bases de polarisation conjuguées peuvent être utilisées. Elles s'excluent donc mutuellement, selon les principes de la mécanique quantique. Pour chaque photon, la base de polarisation est choisie au hasard (avec la probabilité 0,5). Sur le canal quantique, le destinataire autorisé lit les photons en choisissant aussi les bases de lecture au hasard. Puis, sur le canal classique, il informe l'émetteur du choix de ses bases. Celui-ci lui répond en indiquant quelles sont les bonnes bases, c'est-à-dire

celles pour lesquelles leurs choix coïncident. Ils obtiennent ainsi une information commune secrète, correspondant aux photons dont les bases coïncident. Un intrus qui aurait cherché à intercepter la communication aurait détruit l'information en effectuant la mesure et une statistique assez simple sur le succès de la transmission devrait permettre de découvrir cette intrusion.

Les premiers systèmes de cryptographie quantique sur fibre optique commencent à paraître : ils permettent des échanges sur une cinquantaine de kilomètres.

11. – **L'ordinateur quantique et la cryptographie.**

Dans les ordinateurs actuels, chaque composant binaire contient (on pourrait dire : par définition !) un chiffre binaire, ou bit, car un composant ne peut être que dans l'un des deux états (représentés par les chiffres 0 et 1) qu'il est susceptible de prendre. Les opérations de calcul ne traitent donc qu'une configuration binaire à la fois (même si elles portent sur plusieurs bits en parallèle).

Mais la mécanique quantique définit des états particuliers que l'on appelle **états quantiques,** qui consistent pour un même composant binaire à être **simultanément** dans ses deux états : c'est le principe de la **superposition** des états quantiques (par opposition aux **états classiques** non superposés), tant qu'une mesure n'est pas effectuée pour séparer ces états superposés.

L'idée de l'ordinateur quantique [40] repose sur la possibilité de coder simultanément les bits 0 et 1 en un seul état quantique superposé, avec la probabilité 0,5 pour chacun d'eux (ce sont des bits quantiques ou qubits) [41]. Quand un état superposé intervient dans un calcul quantique, les deux valeurs 0 et 1

---

[40] D. DEUTSCH, « Quantum theory, the Church-Turing principle and the universal quantum computer », *Proc. R. Soc. Lond.*, A 400, 1985, p. 97.

[41] Notons qu'en utilisant des noyaux d'indium 113, l'information pourrait être codée directement en décimal. Ces noyaux, dont le spin vaut 9/2, possèdent, en effet, dix états distincts. On reviendrait ainsi tout naturellement au calcul décimal ordinaire !

provoquent simultanément les deux calculs correspondants. Si donc « n » états binaires superposés sont traités au cours d'une opération cela provoque « 2^n » calculs simultanés : il s'agit d'un nouveau type de calcul parallèle, que l'on peut appeler « parallélisme quantique ». De cela résulte la puissance potentielle de ce principe. Cette idée, qui est sans rapport avec la cryptographie quantique présentée au paragraphe précédent, avait déjà été proposée en 1962 par le physicien Richard FEYNMAN.

Comme nous l'avons expliqué au paragraphe 7 ci-dessus, une attaque systématique d'un système de chiffrement dont les clés ont une longueur de « m » bits nécessite « 2^m » étapes de calculs avec un ordinateur classique : si m vaut 128, cela représente plus de 10^{38} opérations, et cette quantité de calculs est définitivement hors de portée de toute machine classique. Par contre un ordinateur quantique pourrait réaliser cette attaque en une seule opération [42].

Mais en réalité, maintenir un composant quantique dans 2^m états superposés semble irréalisable dès que m dépasse quelques unités (même en ajoutant beaucoup de redondance), car il est impossible de les discriminer avant qu'ils ne perdent leur cohérence (le composant redevient alors spontanément classique) et l'information est perdue. En fait un ordinateur quantique s'apparente beaucoup aux calculateurs analogiques d'autrefois : comme ces derniers, il remplace les calculs d'un algorithme de résolution d'une équation par la mesure de l'état d'un système physique ayant le même comportement que celui décrit par cette équation (ici il s'agit de l'équation de Schrödinger, fondement de la mécanique quantique, qui régit le comportement de tous les systèmes quantiques). Et il est sujet aux mêmes limitations : précision limitée, extrême sensibilité au bruit.

En conclusion, cette idée si séduisante sur un plan théorique, ne semble pas présenter une menace sérieuse pour la sécurité des systèmes cryptographiques.

---

[42] En août 2000, le centre de recherche d'IBM à Almaden, a réussi à effectuer un calcul sur 7 bits quantiques pour factoriser le nombre 15 en 5 et 3 !

ANNEXE II

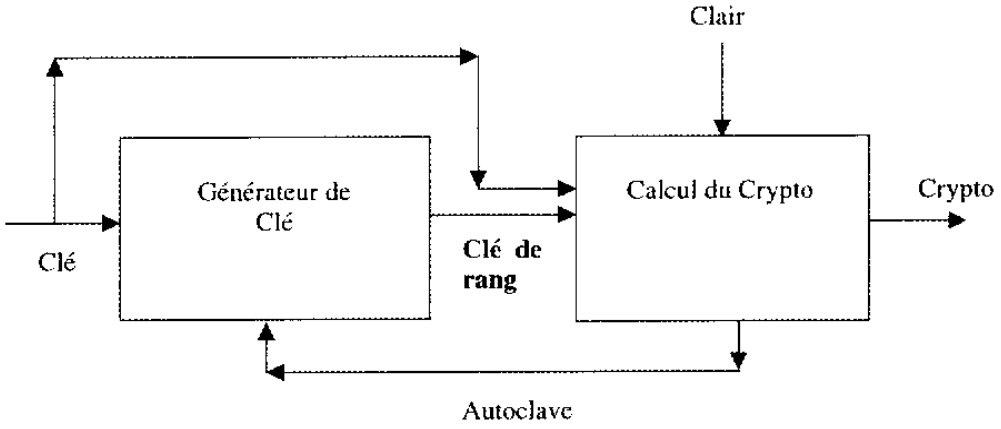
LES PRINCIPES DE MYOSOTIS

1. – La conception de Myosotis.

Les principes qui ont guidé la conception de Myosotis étaient de s'appuyer sur la technologie électronique pour satisfaire deux exigences :

- élaborer une logique de chiffrement constituant la meilleure « approximation » possible du secret parfait (voir le paragraphe 6 de l'annexe I) ;
- rendre les opérations de chiffrement et de déchiffrement aussi automatiques que possible de façon à minimiser l'intervention des opérateurs et ainsi éviter les erreurs et fautes de chiffrement qui étaient fréquentes avec les moyens de cryptologie antérieurs.

Pour répondre à la première exigence, l'idée de Jean-Pierre VASSEUR était d'associer un générateur de pseudo-aléa (ou générateur de clé de rang) au procédé de calcul du crypto proposé par GAUBERT, le tout étant couplé par un dispositif d'autoclave (cf. le paragraphe 6 de l'annexe I). Le schéma suivant décrit la structure logique de Myosotis :



Mais l'autoclave augmente, en général, le nombre d'erreurs de transmission : dans le cas de Myosotis, « n » caractères

consécutifs mal reçus peuvent se traduire par n+1 caractères consécutifs mal déchiffrés, donc erronés (en réalité le nombre de caractères déchiffrés erronés était aléatoire et ne pouvait dépasser n+1). C'est pourquoi l'autoclave était optionnel : il était mis hors service sur les liaisons particulièrement mauvaises pour éviter de les dégrader.

Selon ce procédé, chaque alphabet de chiffrement est obtenu par « l'alignement » dans leur ordre d'arrivée des caractères distincts provenant de la suite de lettres engendrées par le générateur pseudo-aléatoire (clé de rang). La longueur de cette suite a été fixée à 127 éléments (en fait seuls 125 caractères sont utilisés pour créer l'alphabet chiffrant, car les deux premiers étaient utilisés pour le rebouclage de la sortie du générateur d'aléa vers le premier étage (se reporter au paragraphe 2.1). Cela signifie que pour chiffrer un bit clair, 127 bits secrets sont utilisés. C'est la valeur très élevée de ce rapport qui fait la force de Myosotis. D'ailleurs, par la suite, pour aucune machine à chiffrer, on ne pourra réaliser une telle performance.

Pour répondre à la seconde exigence, les fonctions d'exploitation ont été automatisées grâce à un bloc de commande qui permettait de piloter Myosotis. Ce bloc était adapté aux différents modes d'utilisation de la machine ; ces modes étaient facilement sélectionnables à l'aide d'un ensemble de commutateurs.

D'autre part, plusieurs alarmes visuelles et auditives ont été incorporées à Myosotis pour signaler à l'opérateur toutes les anomalies et dysfonctionnements pouvant compromettre la sécurité du système. Certaines détectaient un début de dégradation du fonctionnement de sorte qu'il était possible d'y remédier avant que la panne ne soit devenue dangereuse. Ces alarmes étaient basées sur les propriétés statistiques de Myosotis ; elles se contrôlaient mutuellement (l'alarme principale comportait son propre test de bon fonctionnement) et l'opérateur était informé en continu du bon fonctionnement de la machine. Ainsi, si une panne se produisait, celui-ci pouvait intervenir très rapidement.

La mise à la clé du jour était définie par des petits circuits imprimés (« permutateurs ») que l'on enfichait dans des connecteurs prévus à cet effet. Ces permutateurs étaient munis de détrompeurs, ce qui éliminait toute possibilité d'erreur. Cette mise à la clé était facilitée par l'utilisation de paniers d'enfichage qui permettaient de préparer les clés à l'avance et à l'extérieur de la machine selon l'arrangement prescrit par la liste du jour. Ils étaient mis en place en quelques secondes. Un petit coffret, qui pouvait être plombé, renfermait ces circuits ainsi que deux paniers.

Le chiffrement à l'émission était automatique sans possibilité de fausse manœuvre dangereuse et l'émission directe du clair sur la ligne était impossible [43]. Le déchiffrement à la réception ne nécessitait pas l'intervention d'un opérateur.

La machine admettait deux modes de fonctionnement :

- le mode en ligne, dans lequel elle transmettait le crypto en même temps qu'elle traduisait le message ;
- le mode hors ligne dans lequel elle produisait localement le crypto qui était ensuite envoyé par un appareil conventionnel.

La clé de message (ou marquant de « phase initiale ») était produite par un générateur d'aléa interne et était créée automatiquement à l'émission dans le mode en ligne. Elle pouvait aussi être choisie dans une liste et introduite localement dans le mode hors ligne.

---

[43] En fait, la transmission en clair était possible, car nécessaire pour certaines prises de contact ; mais il fallait à tout prix empêcher la transmission en clair d'un message confidentiel. Pour éviter qu'un opérateur ne conserve indûment ce mode de transmission en clair au moment du chiffrement, il devait appuyer en permanence sur un bouton pour transmettre du clair. Mais ceci l'obligeait à taper le texte d'une seule main. Certains opérateurs ont alors vite trouvé qu'il était facile de passer une règle entre les deux poignées de transport de la machine puis de coincer une gomme entre cette règle et le bouton. On pouvait alors taper avec les deux mains, mais la sécurité était neutralisée. Comme quoi la sécurité repose, *in fine*, sur les hommes et les meilleurs systèmes ne sont bons que s'ils sont bien utilisés !

2. – La constitution physique d'un ensemble Myosotis.

Physiquement un ensemble Myosotis comprenait un bloc chiffrant et un bloc de commande, reliés par un câble multiconducteurs. Différents types de blocs de commande ont été réalisés.

La technologie était à base de transistors au germanium (les composants au silicium n'étant pas encore disponibles) et nécessitait une ventilation forcée pour tenir les objectifs de température. Ce problème thermique était d'autant plus difficile à résoudre que les transistors au germanium étaient très sensibles à la température, que la boîte devait être étanche et que l'armée était très exigeante sur les conditions d'ambiance.

À titre indicatif voici les caractéristiques physiques de cette version de Myosotis, avec les protections électriques et radioélectriques (fusibles, filtres) :

ENSEMBLES	LARGEUR (mm)	HAUTEUR (mm)	PROFONDEUR (mm)	POIDS (kg)
Bloc de chiffrement	455	340	370	48
Bloc de commande	200	390	420	19

Le bloc chiffrant contenait les circuits électroniques nécessaires à la génération de la suite des caractères pseudo aléatoires et au traitement de l'information c'est-à-dire au calcul du chiffrement à l'émission et du déchiffrement à la réception. Il était piloté par une horloge dont la fréquence était de l'ordre de 1 MHz. Le coffret comportait 40 circuits imprimés, soit 1 000 transistors et 4 000 diodes.

Le bloc de commande assurait l'interconnexion du bloc chiffrant avec la voie de transmission et les terminaux associés (téléimprimeurs, transmetteurs automatiques, etc.). Il regroupait les dispositifs de transmission, l'ensemble de synchronisation (caractères et messages devaient être synchronisés) et les différentes commandes d'exploitation mises à la disposition de l'opérateur ainsi que les diverses alarmes et les divers contrôles de bon fonctionnement.

Comme on l'a déjà dit, le rôle de l'opérateur était limité à quelques opérations simples telles que :

- mise à la clé périodique du bloc chiffrant par enfichage manuel direct des permutateurs, sorte de cartes précâblées enfichables, selon les indications d'une liste de clés diffusée par le gestionnaire du réseau de chiffrement, ou par la mise en place des paniers préparés ;
- appui fugitif sur un bouton poussoir déclenchant automatiquement l'établissement de la liaison chiffrée ; cette opération n'est effectuée qu'une seule fois lorsque la liaison est exploitée en chiffrement (continu) de voie et que les équipements d'extrémités restent en synchronisme ; sinon elle est répétée à chaque message si l'exploitation est faite en chiffrement de messages.

Des verrouillages entre les différentes commandes interdisent toute fausse manœuvre dangereuse de l'opérateur et une procédure simple permet d'effectuer rapidement le test général de bon fonctionnement du système Myosotis.

3. – **Le bloc chiffrant : le générateur de clé et le calcul du cryptogramme.**

3.1. – *Le générateur de clé.*

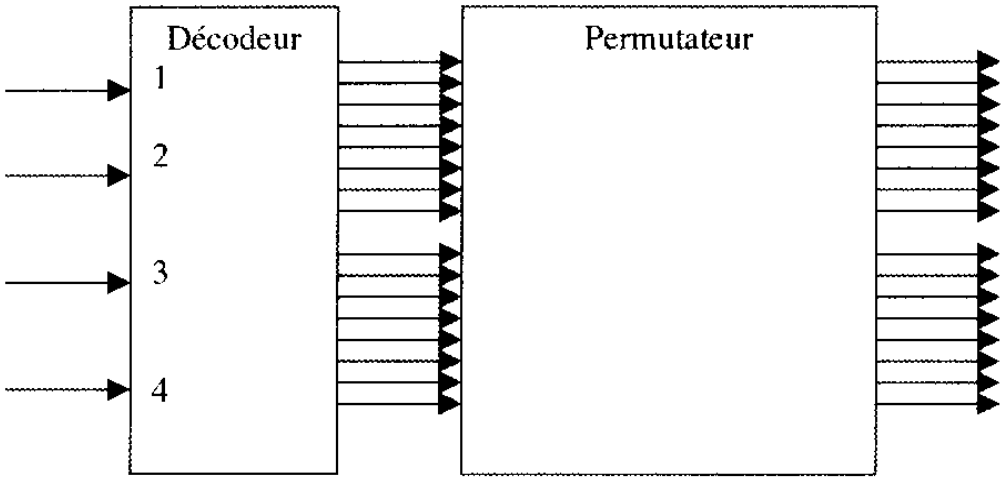
Le rôle du générateur de clé était de fournir à chaque pas du chiffrement une suite pseudo aléatoire de 127 caractères à partir de laquelle était construit l'alphabet de substitution utilisé.

Il se présentait comme un empilement de plusieurs ensembles de circuits se commandant mutuellement. Ces ensembles étaient appelés « étages » en raison de cette structure en pile du générateur. Chaque étage comportait :

- des compteurs binaires dont l'avance est contrôlée par l'étage précédent ;
- des générateurs d'avance de l'étage suivant.

Ces générateurs d'avance contenaient des blocs décodeurs-permutateurs suivis de portes logiques combinant plusieurs sorties

binaires de ces blocs. Ces blocs décodeurs-permutateurs permettaient de réaliser toutes les permutations d'ordre 16 (il y en a 16 !, soit $2{,}1.10^{13}$ environ). La structure d'un tel bloc était la suivante :



Les compteurs du premier étage avancent régulièrement et constituent ce que nous appelons « le moteur » de la clé. Les sorties des compteurs du dernier étage (5 bits en parallèle) fournissent la suite pseudo-aléatoire de 127 caractères. Mais cette sortie influence aussi le premier étage.

L'étude mathématique d'une telle machine est très difficile et pratiquement inextricable. En effet, si chaque ensemble du générateur est à peu près analysable, le tout est impossible à analyser à cause des rebouclages internes et des avances irrégulières de l'horloge. On se heurte très vite à la complexité (exponentielle) des calculs !

Cependant, pour pouvoir estimer le niveau de sécurité du générateur, il est primordial de déterminer sa période qui est un paramètre cryptologique fondamental. D'un point de vue mathématique, le générateur est un automate fini, c'est-à-dire que son nombre d'états internes est borné. Son comportement est donc périodique.

Un premier calcul approximatif montre que la période de la machine comporte au minimum $3{,}19.10^{9}$ états distincts. C'est la période P_{mr} du moteur. Cette période minimale représente dix ans de trafic continu à 75 bauds. Cette valeur paraît déjà

confortable, compte tenu du fait qu'il était prévu de changer la clé toutes les vingt-quatre heures (rappelons qu'une nouvelle clé définit en fait une nouvelle machine !). Cependant, étant donné le fonctionnement irrégulier des autres étages de la machine, la période réelle est une variable aléatoire (dépendant de la clé) dont la valeur moyenne P_m est supérieure à cette valeur d'environ un facteur mille (10^3), soit 3.10^{12} ; et sa valeur maximale est 10^{17}. Cette période maximale, qui est toutefois extrêmement peu probable, représente le nombre total des états de Myosotis, c'est-à-dire le produit du nombre d'états du moteur par le nombre d'états des autres étages (soit $3{,}2.10^7$).

Ces calculs ont soulevé beaucoup de discussions et même donné lieu à des polémiques entre les différents experts ayant participé à l'évaluation de Myosotis, car les calculs exacts étant impossibles, il fallait faire des hypothèses simplificatrices très approximatives et quelquefois contradictoires [44].

---

[44] Le raisonnement suivant fournit l'ordre de grandeur de la période moyenne P_m. Soit $Q = 3{,}2.10^7$, le nombre d'états des étages autres que ceux du moteur. Quand celui-ci a parcouru une période à un instant « i », les autres étages sont dans un état « e_i ». Considérons cette suite d'états :

$$e_1 \rightarrow e_2 \rightarrow \ldots \rightarrow e_i \rightarrow \ldots \rightarrow e_{r-1} \rightarrow e_r.$$

La machine entre dans une période à l'instant « r » s'il existe dans cette suite un état antérieur e_j tel que $e_{r+1} = e_j$, puisqu'à ce moment l'état total de la machine est identique à celui qu'elle avait à l'instant « j ». La probabilité pour que e_{r+1} soit identique à un état antérieur e_j est d'une valeur raisonnable (disons, supérieure à 10 %) dès que le nombre de couples (e_i, e_k) dépasse le dixième du nombre d'états « Q » (loi de Poisson de moyenne 0,1), soit : $r(r-1)/2 > 0{,}1.Q$ ou approximativement $r > 0{,}45.\sqrt{Q}$.

Et la longueur moyenne du rebouclage est la moitié de la longueur de cette suite : $0{,}22.\sqrt{Q}$.

La période correspondante de la machine est alors : $P' = 0{,}22.P_{mr}.\sqrt{Q}$. P' est *a priori* inférieure à la moyenne puisqu'elle a neuf chances sur dix d'être dépassée.

Un calcul plus précis de la période moyenne Pm donne $P_m = P_{mr}.\sum_r r.P(r)$, où P(r) est la probabilité que $e_{r+1} = e_j$, soit $P_r = (r/Q^r).(Q-1)!/(Q-r)!$ On obtient la valeur approchée : $P_m = \sqrt{(\pi/8)}.P_{mr}.\sqrt{Q}$, soit : $P_m = 0{,}627.P_{mr}.\sqrt{Q}$.

Cette formule en $\sqrt{Q}$ a été confirmée quelques années plus tard (1972) par le théorème de D. KNUTH, N.G. de BRUIJN, S. RICE sur la hauteur moyenne des arbres aléatoires.

Il était impossible à l'époque de réaliser une vérification expérimentale de ces formules, tout au moins pour des machines ayant la complexité de celle de Myosotis. Tout ce que l'on peut dire, c'est que les résultats de l'étude statistique ont permis d'affirmer que la période était beaucoup plus grande que 10^9.

Les permutateurs de rang 16 des blocs décodeurs-permutateurs constituaient les éléments secrets variables internes. Ils se présentaient sous forme de cartes de circuits imprimés précâblés, définissant une permutation d'ordre 16. On pouvait les enficher selon quatre positions différentes. Quatorze de ces permutateurs servaient à définir la structure interne de Myosotis, tandis que sept autres servaient à définir l'état initial de la machine. Les mêmes permutateurs pouvaient être utilisés indifféremment pour la structure interne ou l'état initial de la machine. Au total 21 permutateurs devaient être utilisés pour configurer une machine.

C'est sur le choix de ces 21 permutateurs, effectué dans un lot de 30, que reposait le secret de la machine pour une période donnée, dite **crypto-période** (en général la durée d'une crypto-période est de vingt-quatre heures). Comme toutes ces positions définissent des configurations différentes, le nombre total de clés distinctes que Myosotis peut recevoir est donc :

$$K = A^{21}_{30}.4^{21} \text{ soit } 3{,}21.10^{39}.$$

Toutes ces clés étant équiprobables, leur entropie est :

$$H(K) = \log_2 (K) = 131{,}7.$$

C'est-à-dire que les clés de Myosotis ont une longueur équivalente de 132 bits.

L'initialisation du générateur de clé était différente à chaque message : un mécanisme de sécurité particulier permettait d'éviter que se produisent deux initialisations identiques successives. Cette initialisation était réalisée par le chiffrement d'une séquence de 10 caractères aléatoires (clé de message, produite par le générateur d'aléa interne) ; ce mécanisme permet de définir $32^{10} \# 10^{15}$ clés de message possibles. Les clés de message avaient donc une longueur équivalente de 50 bits.

3.2. – *Le calcul du cryptogramme.*

L'opération réalisée par l'organe de calcul de Myosotis est une substitution. L'équation du chiffrement est simple : si C_i désigne le caractère clair, « i » indiquant son rang dans l'ensemble ordonné que constitue le message, l'automate détermine une substitution S_i appartenant aux 32 ! substitutions possibles (ou aux 31 !, ou aux 26 ! si Myosotis travaille respectivement en 31 ou 26 caractères) et la lettre Γ_i correspondante du crypto est donnée par :

$$\Gamma_i = S_i\ (C_i).$$

Au déchiffrement on reconstitue la substitution inverse S_i^{-1}, ce qui donne le clair.

Pratiquement, au chiffrement (ou au déchiffrement) l'ordre des opérations est le suivant :

a) Introduction du caractère clair (ou du caractère chiffré) et émission d'un signal de synchronisation.

b) Le générateur de clé avance de 127 pas et s'arrête. Les 127 caractères qu'il a fournis servent à constituer l'alphabet de substitution ; souvent on obtient un alphabet complet mais pas toujours.

c) Si ça n'est pas le cas, un dispositif de complément d'alphabet entre en fonction après l'arrêt du générateur de clé et ajoute les caractères manquants.

d) Le caractère chiffré (ou le caractère clair) est émis.

Le grand intérêt technologique de Myosotis est de pouvoir chiffrer et déchiffrer à la volée, c'est-à-dire sans avoir à mémoriser l'alphabet chiffrant, les lettres de l'alphabet chiffrant étant simplement comptabilisées dans une mémoire constituée de 32 capacités. Chaque fois que cette mémoire enregistre une nouvelle lettre, elle provoque l'avance d'un compteur. Lors du chiffrement, il suffit de détecter, au cours de la séquence de génération de l'alphabet de chiffrement, la coïncidence entre la lettre du clair et le compteur d'avance pour obtenir le crypto. Lors du déchiffrement, on détecte la coïncidence entre le crypto et le caractère fourni par le générateur de clé pour obtenir le clair

qui est la valeur contenue dans le compteur d'avance. Cette propriété assure une économie de matériel et une simplicité de réalisation très appréciable.

Mais la grande force cryptographique de Myosotis est sa capacité de résistance à la cryptanalyse basée sur les **messages parallèles,** c'est-à-dire des messages qui comportent des séquences de lettres qui ont été chiffrées avec la même suite de clés de rang. On dit que les clés utilisées pour produire ces messages sont en **recouvrement :**

- la longueur « L » de cette séquence est la longueur du recouvrement ;
- le nombre « P » de messages parallèles est la profondeur du recouvrement.

Le nombre dangereux de messages parallèles (c'est-à-dire la valeur que ne doit pas dépasser « P ») a été estimé [45] à 15 (pour les langues usuelles). La probabilité que Myosotis produise 15 messages parallèles au cours d'une crypto-période est absolument négligeable. En outre, il aurait été extrêmement difficile de détecter un ensemble d'au moins 15 messages parallèles dans le flot du trafic de Myosotis : cela aurait représenté un travail gigantesque : Myosotis n'était pas attaquable par les messages parallèles.

Le chiffrement d'un caractère télégraphique s'effectue en 2 ms ; il est donc possible de chiffrer ou de déchiffrer 2 500 bits en une seconde ce qui correspond à un débit d'information de 2 500 bauds (sans « start », ni « stop »).

La vitesse de Myosotis permet de l'adapter au chiffrement d'octets, mais alors le chiffrement doit s'effectuer en deux séquences, l'une effectuant le traitement des cinq premiers bits, l'autre le chiffrement des trois bits restants. Le traitement d'un caractère de huit bits prend donc 4 ms ; la vitesse est alors de 2 000 bits/s.

[45] Cette estimation était très prudente, puisque la valeur théorique donnée au paragraphe 6 de l'annexe I est au moins deux fois plus élevée.

4. – **Les blocs de commande.**

Tous les contrôles d'exploitation de Myosotis sont rassemblés dans le bloc de commande. Celui-ci comprend de nombreux automatismes ce qui rend son utilisation très simple et qui peut être assurée par du personnel non spécialisé. Sur la face avant, des boutons de contrôles divers permettent de sélectionner les différents modes d'exploitation.

Le bloc de commande pouvait être utilisé seul ou en liaison avec un bloc de télécommande, plus petit et plus léger (2 kg) que le bloc de commande. Celui-ci reproduisait exactement les mêmes fonctions que le bloc de commande. Le bloc de télécommande pouvait être éloigné de 150 m du système Myosotis.

4.1. – *Les liaisons télégraphiques.*

Plusieurs blocs de commande ont été étudiés.

a) Le bloc de commande télégraphique standard conçu pour fonctionner avec n'importe quel type d'équipement télégraphique terminal conforme aux normes CCITT, aux vitesses de 45,5, 50, 75 ou 100 bauds. Les dispositifs de transmission télégraphique sont contenus dans le bloc qui se connecte directement à une ligne télégraphique ou à un émetteur récepteur radio. Il permet le chiffrement d'alphabets à 32, 31 et 26 caractères.

Le trafic à 31 caractères est prévu pour le télex international qui n'autorise pas l'emploi du 32^{e} caractère. Le trafic à 26 caractères est prévu au cas où l'on désire que le message (chiffré) soit composé uniquement de lettres. Ces messages sont automatiquement formatés en groupes de cinq lettres.

Un ensemble de cavaliers sur une plaquette de connexion permet le choix du mode de trafic (simplex, alternat, duplex, réseau conférence, diffusion) et l'utilisation de tous les standards usuels (24 ou 48 volts, simple ou double courant, deux ou quatre fils, polarité normale ou inversée).

Le dispositif de synchronisation a deux modes de fonctionnement :

- le mode asservi, où le synchronisme se maintient tant que la liaison reste établie et, en cas de coupure de la ligne, reste maintenu au moins trente minutes ;
- le mode libre, où l'horloge de réception est indépendante des signaux reçus et des oscillateurs de très haute stabilité permettent de conserver le synchronisme plusieurs semaines.

b) Les blocs de commande télégraphiques hors ligne, conçus et réalisés par la SAGEM, pour l'armée de l'Air. Deux variantes ont été étudiées :

- le bloc à grande vitesse. Associé à un lecteur et un perforateur de bandes rapide, ce bloc peut chiffrer à 100 ou 150 caractères par secondes (le bloc de chiffrement lui-même permettait de chiffrer jusqu'à 500 caractères par secondes) ;
- le bloc à basse vitesse. Associé à un téléimprimeur, ce bloc a des performances comparables au bloc standard dans son emploi hors ligne, mais il ne dispose pas du chiffrement à 26 caractères.

c) Le bloc de commande télégraphique simplex rapide qui permet de chiffrer les caractères à 5 et 8 moments à des vitesses de 600, 1 200, 1 800 et 2 000 bit/s, étudié pour la Marine.

d) Le bloc de commande télégraphique duplex à 5 moments (50, 75 ou 100 bauds) et 8 moments (110 ou 200 bauds).

4.2. – *Les liaisons fac-similé.*

L'ensemble de chiffrement du fac-similé TS 550 comprenait outre le bloc chiffrant Myosotis, un bloc de commande adapté au fac-similé TF-TF-2C de la CIT, les lettres étant considérées comme une suite de bits. La vitesse de transmission était de 1 800 bits/s ou de 2 400 bits/s, ce qui permettait, à l'aide de modems SAT, de transmettre sur les liaisons téléphoniques normales des images chiffrées en noir et blanc de documents aux

formats 21 × 27 ou 21 × 29. Cependant, ce matériel n'a pas fait l'objet d'un développement de série.

4.3. – *La téléphonie de haute sécurité.*

Un bloc de commande a été conçu pour le chiffrement de la téléphonie après réduction de bande et numérisation du signal vocal par un vocodeur à 2 400 bits/s.

Un ensemble de cryptophonie de haute sécurité comprenait à chaque extrémité un bloc chiffrant Myosotis avec un bloc de commande adapté, un vocodeur et un modem. Le modem était de type classique pour les transmissions sur voie filaire ou équivalente et d'un type spécial (KINEPLEX) pour les voies radio à grande distance. L'ensemble pouvait être exploité en duplex (sur une ligne de 4 fils ou sur deux lignes de 2 fils) ou en alternat (sur une ligne de 2 fils).

Ce matériel aurait équipé en priorité le réseau gouvernemental de haute sécurité mais la France ne disposait pas de vocodeur de grande qualité et le volume de l'ensemble paraissait prohibitif de sorte que les études de cryptophonie ont perduré en France jusqu'aux années quatre-vingt-dix. Il faut dire qu'à cette époque, les autorités gouvernementales étaient difficiles à convaincre de l'intérêt de chiffrer les liaisons téléphoniques, malgré les actions au plus haut niveau que le STCCh menait en ce domaine.

ANNEXE III

DEUX ANECDOTES CONCERNANT MYOSOTIS

Préambule.

Ces deux anecdotes, rapportées par Xavier AMEIL, constituent une certaine illustration de la gestion du secret. L'anecdote de Moscou montre que si le secret exige les matériels les plus perfectionnés, celui-ci repose en définitive sur les hommes dont toutes les actions doivent être méticuleusement identifiées, analysées et contrôlées. L'anecdote de La Nouvelle-Orléans montre que la consigne de considérer comme confidentiel le nom de Myosotis, s'est maintenue pendant plusieurs années.

1. – Moscou.

Lors de l'affaire d'espionnage Farewell [46], à laquelle j'ai été mêlé à Moscou du début mars 1981 à fin mai 1981, le colonel FERRAND, qui avait pris ma suite pour assurer la liaison avec la taupe [47] soviétique, membre du KGB, me demande de venir à l'ambassade de France.

Il me reçoit dans une enceinte ultra-protégée, y compris par une cage de Faraday, et où se trouvait une machine dérivée de Myosotis. Cette machine servait uniquement à Monsieur l'Ambassadeur. Celui-ci avait l'habitude de taper lui-même en clair les messages secrets qu'il envoyait à Paris, après chiffrement par cette machine.

Le but de cet entretien était de m'annoncer que la taupe avait disparu depuis le 15 janvier 1982 et que la rencontre de rappel du 31 janvier n'avait rien donné.

J'ai commencé par ce préambule pour montrer le luxe de précautions que Monsieur l'Ambassadeur prenait pour envoyer

---

[46] Cette affaire est racontée dans le livre de Sergueï KOSTINE, *Bonjour, Farewell*, Paris, Robert Laffont, 1997.

[47] Il s'agit de Vladimir VETROV, dont Farewell était le nom de code.

ses messages. Malheureusement, il ne se doutait pas que sous la machine était dissimulée une sorte de condensateur piégé contenant des dérivations qui permettaient de renvoyer directement les signaux en clair sur des fils électriques qui alimentaient aussi un petit bâtiment du ministère de l'intérieur soviétique, voisin de l'ambassade.

Cette supercherie ne fut découverte qu'en mars 1983, lorsqu'un chiffreur de Moscou fut obligé de changer une machine (sans doute à cause d'une panne). Pendant qu'il travaillait, il fit tomber un gros élément recouvert de plastique. Il eut la présence d'esprit de renvoyer le tout à Paris, où le piège fut mis à jour. On découvrit alors que la deuxième machine Myosotis était piégée de la même manière.

Apprenant cet incident, le président MITTERRAND furieux, après quelques hésitations, prit la décision de renvoyer quarante-sept diplomates soviétiques de l'ambassade parisienne. Les noms de ces diplomates avaient été fournis par la taupe comme étant des espions.

Malheureusement, ce renvoi permit au KGB d'identifier la personne qui avait établi cette liste ; et ils décidèrent de l'arrêter pour trahison. Cependant, celui-ci était déjà en prison où il purgeait une peine pour le meurtre d'un milicien. Il fut exécuté en janvier 1984.

On se rendit compte ensuite que cette manipulation sur les deux machines Myosotis n'avait pu être réalisée que lors du passage de la frontière polono-soviétique, les douaniers ayant exigé un arrêt de vingt-quatre heures pour formalités. C'est pendant cet arrêt que les Soviétiques ont dû mettre à profit un défaut de surveillance, pour intervenir sur les machines, qui pourtant faisaient partie de la valise diplomatique !

2. – La Nouvelle-Orléans.

Je suis allé voir en 1992 ma fille et mon gendre qui était consul général à La Nouvelle-Orléans. Lors d'une visite au consulat, j'ai demandé à voir l'installation du système de chiffrement. Le chiffreur m'a montré un appareil de faibles

dimensions, très compact, qui n'avait rien à voir avec les premières machines Myosotis. En fait, il s'agissait d'une nouvelle version de Myosotis de taille beaucoup plus petite en raison de l'emploi de circuits intégrés. Je lui parlais alors de Myosotis, et il parut très étonné que je prononce ce nom, car il avait pris l'engagement de ne jamais prononcer ce mot devant des personnes qui n'étaient pas censées le connaître !

Xavier AMEIL.

Commentaires (concernant l'anecdote de Moscou) du colonel André CATTIEUW.

L'anecdote rapportée par M. AMEIL m'amène à préciser quelques points puisque le Service Technique Central des Chiffres et de la Sécurité des Télécommunications (SCCST), que je dirigeais à l'époque, a été mêlé d'assez près à cette affaire. En janvier 1983, le 11 janvier si je me souviens bien, l'ambassade de France à Moscou signalait au Quai d'Orsay à Paris que son service du chiffre venait de découvrir des dispositifs d'écoute clandestins dans certains de ses téléimprimeurs associés à la machine à chiffrer Myosotis, ces téléimprimeurs étant en service depuis au moins six ans à Moscou. Les Affaires étrangères ont alors demandé l'expertise du SCCST pour analyser le piégeage décelé tout à fait par hasard par un des chiffreurs de l'ambassade. Celui-ci, un peu bricoleur, avait, contrairement aux consignes reçues (car les opérateurs ne font pas d'entretien), soulevé le capot d'un téléimprimeur Sagem associé à une Myosotis et avait été surpris de constater que des fils électriques bizarres sortaient du condensateur dont trois fils bleu, blanc et rouge (... voyez l'humour des Soviétiques !). Poussant plus loin, il s'était aperçu que le condensateur renfermait de l'électronique qui n'aurait pas dû y être... L'un des matériels en cause fut rapidement rapatrié et analysé au SCCST. Il ne fut pas difficile de constater que l'électronique en question servait à capter le clair avant chiffrement ou après déchiffrement et à l'envoyer sur le circuit d'alimentation électrique à l'aide d'une fréquence passant sous la fréquence de coupure du filtre de protection. Les Affaires étrangères s'aperçurent bien

vite que la plupart de leurs téléimprimeurs étaient ainsi piégés y compris ceux du poste diplomatique de Leningrad. Comme le dit M. AMEIL, la faille résidait, selon ce qu'on m'en a dit, dans le fait qu'il y avait rupture de charge, et donc de surveillance du matériel, en cours de transport. Personne ne s'en était rendu compte au préalable, la valise diplomatique étant confiée à un transporteur civil sans être accompagnée par un agent du Quai d'Orsay.

Je me souviens avoir informé le secrétaire général du gouvernement de cette affaire et du rôle joué par le SCCST dans l'analyse du piège. Peu porté sur les questions secrètes, surtout sur celles qui sentaient le souffre des services spéciaux, il m'a écouté avec un rien d'impatience qui se mua en stupéfaction étonnée lorsque je lui ai indiqué que, selon l'ancienneté des pièges, on pouvait être sûr que, lors de leur réunion de mai 1980, M. Leonid BREJNEV connaissait à l'avance le dossier de M. GISCARD D'ESTAING et les intentions françaises par les messages échangés entre Paris et l'ambassade de France à Moscou et avait donc pu manœuvrer à son aise au cours des discussions. J'ajoutai qu'il entendrait probablement parler de cette affaire à l'Élysée que M. CHEYSSON n'avait pas dû manquer d'aviser... Ce qui fut le cas... puisque quelques jours plus tard, le secrétaire général me donnait une liste de très hautes personnalités en me demandant de les informer personnellement de cette affaire en toute discrétion.

Comme dans tout incident, il y a eu des signes prémonitoires qui auraient dû avertir du risque mais que l'on comprend après coup. Comme le dit M. AMEIL, il y a eu une commande par les Soviétiques de plusieurs centaines de condensateurs SAGEM. Elle a intrigué le SGDN et le SCCST qui n'ont pas jugé utile de s'opposer à cette exportation tout en s'interrogeant sur la raison de cette commande. Il y a eu aussi l'avertissement fait par la DGSE à la réunion de la sous-commission « Cryptologie » du 10 février 1971, soit relativement peu de temps avant la pose des pièges, qui mettait en garde contre la pose de dispositifs d'écoute russes incorporés d'une manière invisible dans un téléimprimeur en usine ou en cours de transport pour retransmettre vers l'extérieur les informations détectées...

Enfin, il faut dire que nous n'avons pas été les seuls à être pris à ce jeu : la NSA américaine, avertie par la DGSE et le SCCST, a fait procéder à une vérification de ses équipements pour constater qu'ils étaient piégés eux aussi à un point tel que les Américains ont dû prendre la décision de rapatrier et de remplacer systématiquement tous les équipements électriques ou électroniques (téléimprimeurs, machines à chiffrer, machines à écrire, etc.) de leurs postes diplomatiques de l'autre côté du rideau de fer. Au-delà des pièges très astucieux qu'ils découvraient les Américains étaient vexés de constater que les circuits électroniques utilisés par les Soviétiques avaient été achetés... aux États-Unis.

J'ajoute, enfin, que dans l'entretien du général ANDREYEV avec David KAHN, objet de l'article « Soviet COMINT in the cold war » paru dans la revue *Cryptologia* de janvier 1998, cet ancien responsable du COMINT [48] soviétique explique qu'au cours de la guerre froide, l'URSS ne cherchait à décrypter que le trafic des ambassades qui utilisaient, à Moscou, des produits commerciaux ; pour les autres, le décryptement était abandonné car trop difficile ou impossible et l'effort était mis sur le piégeage électronique.

[48] COMINT signifie « Communication Intelligence », c'est-à-dire « Renseignements obtenus à partir de sources de Télécommunications ».

ANNEXE IV

LA NOTION DE SUITES ALÉATOIRES

1. – Le problème de la caractérisation des suites aléatoires.

Considérons les deux suites suivantes, décrivant chacune une succession de 20 tirages du jeu à Pile (P) ou Face (F) :

(S1) P F P F P F P F P F P F P F P F P F P F
(S2) P F P P F F P F F F P P P P F P F P P F

Si l'on parie lors de ces tirages, on constate qu'avec la suite S1 il est facile de gagner : Face sort lors des tirages pairs et Pile, lors des tirages impairs. Par contre, il ne semble pas qu'il existe une méthode analogue pour gagner souvent avec la suite S2. La suite S1 ne peut donc être considérée comme aléatoire, alors que S2 semble l'être. Ainsi une statistique simple du couple « P, F » permet de rejeter l'hypothèse que S1 est aléatoire, alors que pour S2 cela n'est pas évident. Par exemple, dans S2 l'écart de la fréquence de P (11 sur 20 tirages, soit 0,55) avec celle de F (9 sur 20, soit 0,45) n'est pas significatif (la fréquence théorique est 0,5).

Pourtant il existe aussi une méthode pour gagner systématiquement avec S2, mais elle est plus difficile à trouver : à partir du cinquième tirage, il faut parier F si les résultats du tirage immédiatement précédent et du quatrième tirage précédent sont identiques, sinon on parie P. Finalement S2 n'est pas beaucoup plus aléatoire que S1 !

Se pose alors la question suivante : peut-on définir un ensemble de critères effectivement applicables permettant de décider si une suite est ou non aléatoire ?

2. – L'approche statistique de l'aléa.

Cette approche provient d'un grand principe énoncé vers 1930 par R. von MISES :

« Considérons un jeu de hasard comme celui de Pile ou Face (avec une pièce de monnaie non truquée). On observe tous les

tirages, mais on peut choisir de parier ou non, avant chacun d'eux. Ce principe consiste à affirmer que dans une suite (indéfinie) de paris, il n'existe aucune méthode permettant à un parieur de gagner plus souvent qu'une fois sur deux. »

Autrement dit, quelle que soit l'observation des tirages déjà effectués, on ne peut prédire l'issue d'un nouveau tirage avec une probabilité meilleure que 0,5. En fait ce principe est général et on le résume quelques fois très simplement : il n'existe aucune martingale pour gagner dans les jeux de hasard (équitables).

La validité de ce principe exige une définition adéquate des méthodes que l'on envisage pour gagner : ces méthodes doivent être effectives [49] et applicables indéfiniment. Par exemple, celles qui supposeraient que l'on connaisse l'avenir sont exclues : une procédure de décision pour parier au nième tirage ne peut prendre en compte que les résultats des (n-1) premiers tirages. De même les règles définissant la méthode sont fixées au début du jeu.

A contrario, ce principe permet d'affirmer que si une méthode permet de gagner plus souvent que ne le prédit la loi de hasard régissant ce jeu (c'est-à-dire, dans le cas du jeu de Pile ou Face, plus d'une fois sur deux), c'est que les tirages successifs ne sont pas aléatoires. C'est la base des tests statistiques d'aléa (en pratique, on ramène souvent une suite quelconque à une suite binaire, dont les 0 et les 1 sont équiprobables, comme pour le jeu de Pile ou Face).

Les règles de la méthode envisagée permettent de définir un événement E dont la probabilité d'occurrence est parfaitement calculable en fonction de la loi du hasard régissant la suite considérée. Le test consiste à détecter l'occurrence de E (ou à mesurer sa fréquence) dans cette suite et à calculer la probabilité du résultat obtenu dans l'hypothèse où cette suite est vraiment aléatoire. On se donne un seuil de décision « s » (on

[49] Dans cette annexe, le mot « effective » appliqué à fonction, méthode, procédure... signifie « définissable par un algorithme ou un programme ». Il est synonyme de « calculable ».

choisit en général une valeur dont la probabilité qu'elle soit obtenue dans le cas d'une suite aléatoire est de 5 %) :

- si la valeur obtenue est inférieure à « s », on rejette l'hypothèse que la suite est aléatoire ;
- sinon, on ne peut rejeter cette hypothèse.

Les limites de ces méthodes sont évidentes :

- le résultat ne permet pas de décider si la suite est aléatoire ;
- le résultat est fonction de la ou des méthodes choisies.

Des suites vraiment aléatoires risquent d'être rejetées, puisque par définition du seuil « s », le résultat du test d'une suite aléatoire a une probabilité de 5 % d'être en dessous du seuil. Mais, pour les tests appliqués aux machines cryptographiques, l'erreur que l'on veut éviter de faire est d'accepter comme étant aléatoire une suite qui ne l'est pas !

En réalité, la grande difficulté réside dans le choix des méthodes. Une méthode statistique reste grossière et ne permet pas de détecter une loi déterministe ni un événement rare. Il est évident que l'on doit en utiliser un grand nombre et que ces méthodes doivent être assez variées pour couvrir le plus grand nombre de règles imaginables.

En outre ces méthodes doivent être très peu corrélées entre elles, voire indépendantes et non redondantes, car les tests iraient dans le même sens et conduiraient à une mauvaise décision. C'est ce qui explique l'importance et la complexité de l'étude statistique de Myosotis.

Une définition plus précise de ces méthodes fut donnée, vers 1966, par A. KOLMOGOROV lorsque la notion d'algorithme fut formalisée. Dans le cas d'une suite infinie, cette définition conduit à la conclusion qu'il faudrait appliquer tous les tests définis par une fonction effectivement calculable.

Comme il y en a une infinité (dénombrable), on ne peut épuiser tous les tests nécessaires [50].

---

[50] Ceci signifie qu'aucune fonction calculable ne peut simuler le hasard, tant que l'on s'intéresse à des suites aussi longues que l'on veut. Par contre certaines fonctions (comme les fonctions chaotiques) peuvent engendrer des suites qui, sur des périodes plus ou moins courtes, ressemblent beaucoup à de l'aléa.

Constat : cette approche ne peut donner une définition des suites aléatoires, mais elle permet de définir des critères opérationnels pour éliminer les suites qui ont une très faible chance d'avoir été produites par un processus aléatoire.

3. – L'approche algorithmique (ou formelle) de l'aléa.

Cette approche découle d'une analyse de la complexité des suites, due pour l'essentiel à G.-J. CHAITIN (1965). Dans cette théorie, on considère que les suites sont engendrées par des programmes, écrits dans un langage de programmation quelconque mais universel (la plupart des langages sont universels). On définit la taille d'un programme par la longueur de son texte (évalué, par exemple, en nombre de bits). La complexité d'une suite est la taille du plus petit programme qui peut l'engendrer [51].

Une suite est considérée comme « simple » si elle est engendrée par un programme court, comparée à sa longueur, sinon elle est considérée comme « complexe ». L'avantage de cette approche est d'être bien adaptée aux suites finies qui, en pratique, sont les suites qui nous intéressent.

Notons que pour toute suite « S » de longueur l(S), il existe un programme la calculant et dont la longueur est l(S) à une constante additive près : c'est le programme qui consiste à l'imprimer directement. Un tel programme contient essentiellement la suite « S » elle-même et les instructions nécessaires à l'imprimer (ces instructions sont indépendantes de « S » : ce

---

[51] La complexité « c » d'une suite « S » est en réalité indépendante du langage de programmation « L » utilisé. En effet soit « P » un programme calculant « S » dans « L ». Considérons un autre langage « L' ». Comme « L' » est supposé universel, on peut simuler « L » dans « L' » par un interpréteur « I » de « L ». « I » est indépendant de « S ». Soit « i » la taille de cet interpréteur. Dans « L' », un programme calculant « S » est constitué du couple (I,P) dont la taille est : c + i. Donc la complexité de « S » dans « L' » est : c' = c + i. Par un raisonnement symétrique, on a : c = c' + i'. Donc c - i' = c' = c + i : la complexité est la même à une constante additive près qui ne dépend que de « L » et de « L' ».

peut être « imprimer le premier bit, puis chaque bit suivant, jusqu'à épuisement de la suite »). Étant donné une suite, s'il n'existe pas de programme capable de l'engendrer et qui soit plus court qu'elle, c'est que cette suite est d'une complexité maximale. Elle n'est pas, non plus, « prédictible » : il n'existe pas de programme court qui, observant une petite portion de « S », engendre ensuite le reste de la suite. Ce sont de telles suites que l'on a envie de qualifier d'« aléatoires ». Cela revient à considérer que le caractère aléatoire d'une suite provient des informations « indépendantes » qu'elle contient. Mais le nombre de ces informations indépendantes est forcément inférieur à celui que contient un programme capable de l'engendrer.

On pose donc la définition suivante :

Définition : une suite « S » est aléatoire si sa complexité c(S) est de l'ordre de grandeur de sa longueur : $c(S) \approx l(S)$.

Pour démontrer que la complexité d'une suite est supérieure à un nombre « k » donné, on se donne un système formel constitué d'un certain nombre d'axiomes et de règles de déduction. Ceci définit une procédure de preuve de complexité « P ». Or, on peut prouver le résultat suivant [52] :

Théorème : une procédure « P » ne peut montrer que la complexité d'une suite est supérieure à « n » que si : $n \leq c(P)+a$, où « a » est une constante indépendante de la suite.

Par conséquent on ne peut calculer la complexité d'une suite aléatoire beaucoup plus longue que « P ». D'où le corollaire suivant :

Corollaire (indécidabilité de l'aléa) : on ne peut décider si une suite est aléatoire.

---

[52] D'un point de vue équivalent, il n'existe pas de programme capable de calculer, pour tout nombre « k », une suite « s_0 » dont la complexité est supérieure à « k » : $c(s_0)>k$. En effet, supposons qu'un tel programme « P » existe. Cette suite « s_0 » étant engendrée par « P » et la donnée « k », sa complexité est par définition plus petite que $c(P)+c(k)$. Comme c(k) est de l'ordre de $\log_2(k)$, ces deux inégalités sont incompatibles dès lors que « k » est assez grand ; donc « P » n'existe pas.

Constat : cette approche donne une définition mathématique de l'aléa ; mais elle n'est pas opérationnelle pour éliminer les suites non aléatoires (sauf pour des suites trivialement simples).

4. – Statistiques et information : nombre de tests nécessaires.

La notion formelle de l'aléa permet d'expliquer les limites des tests d'aléa.

En effet, un test T_i est défini par un certain ensemble de résultats assortis de leurs probabilités :

$$T_i = \{t_i^j \text{ avec } p_i^j = \text{prob } (t_i^j)/j = 1 \text{ à } m\}.$$

La quantité moyenne d'information apportée par ce test est donnée par son entropie :

$$H(T_i) = -\sum_j p_i^j \log_2 p_i^j.$$

Or un ensemble de tests « T » = $\{T_i/i = 1 \text{ à } N\}$ ne saurait apporter plus d'informations que n'en contient la suite « S » : $\sum i\ H(T_i) \leq c(S)$.

D'un autre côté, pour que ces tests épuisent toute l'information contenue dans la suite, on doit avoir $\sum_i H(T_i) \geq c(S)$. Finalement un ensemble de tests indépendants doit vérifier la relation :

$$\sum_i H(T_i) = c(S).$$

Si la suite est aléatoire $c(S) \approx l(S)$, soit :

$$\sum_i H(T_i) \approx l(S).$$

En général le nombre m de résultats possibles d'un test est de l'ordre de grandeur de la longueur de la suite ($m \approx l(S)$) [53]. Donc $H(T_i)$ est inférieur à $\log_2 m \approx \log_2 l(S)$, et $N \log_2 l(S) \approx l(S)$.

Finalement, le nombre N de tests indépendants doit donc être de l'ordre de :

$$N_0 \approx l(S)/\log_2 l(S).$$

[53] En réalité le nombre « m » est plutôt de l'ordre de grandeur de la racine carrée de l(S). C'est le cas des lois de Gauss dont l'écart-type est égal à (vl(S))/2. Donc N_0 devrait être multiplié par 2.

Ce nombre N_0 est aussi un maximum à ne pas dépasser, sans quoi les tests ne pourraient être indépendants. En cryptographie, on s'intéresse à des suites d'au moins 10^{12} bits et dans ce cas le nombre possible de tests indépendants est : $N_0 \approx 2{,}5.10^{10}$. En pratique, il est impossible de faire autant de tests ; on n'en effectue qu'une infime partie. Il est donc très important de bien les choisir.

Si l'on effectue autant de tests, c'est qu'il n'y a pas de tests « meilleurs » que d'autres et que chaque test apporte un point de vue complémentaire sur les éventuels défauts des suites obtenues. Étant donné le grand nombre de tests utilisés, on n'applique pas de critère de décision à chacun d'eux : il est normal que certains tests soient bons et d'autres mauvais, sans quoi toutes les suites seraient rejetées. Il faut donc être très prudent lors de l'interprétation des résultats, d'autant qu'il est impossible de tenir compte des corrélations pouvant exister entre tous ces tests.

5. – **Les vrais générateurs d'aléa.**

Il existe de nombreux dispositifs physiques dont le comportement est régi par les lois du hasard, c'est-à-dire par des processus aléatoires : la désintégration d'atomes radioactifs, les fluctuations du courant d'une diode, le bruit de fond d'un amplificateur... On peut donc les utiliser pour en faire de véritables générateurs d'aléa : on détecte la fluctuation aléatoire du signal et, en la comparant à un niveau fixé, on obtient un bit (ou un nombre) dont la valeur est aléatoire. On décide arbitrairement que si la valeur mesurée est inférieure à ce niveau on obtient par exemple un « 1 », si elle est supérieure, on obtient un « 0 ». Ce niveau doit être déterminé par la condition que la probabilité que le signal dépasse sa valeur est de 50 %.

Cependant ces dispositifs sont limités par la précision (et aussi la fidélité) des comparateurs qui permettent rarement d'atteindre un écart d'équiprobabilité meilleur que 10^{-5}. Ceci est nettement insuffisant pour les besoins de la cryptographie qui exige une équiprobabilité meilleure que 10^{-12}, voire 10^{-15}. Il est donc nécessaire de les compléter par des mécanismes logiques

qui améliorent leur équiprobabilité. Ces mécanismes sont déterministes. Un mécanisme bien connu est celui proposé par le mathématicien John von NEUMANN, qui fut aussi le concepteur d'un des premiers ordinateurs électroniques. Ce mécanisme consiste à transformer la suite de bits aléatoires « S » en une autre suite « S' » de la manière suivante. On découpe la suite « S » en paquets de deux bits consécutifs et on produit un bit de « S' » si ces deux bits sont différents, sinon aucun bit n'est produit. Le bit produit est « 0 » ou « 1 » selon que le premier bit du couple extrait de « S » est « 0 » ou « 1 ».

Le tableau ci-après résume cette règle :

PAQUETS DE LA SUITE « S »	BITS DE LA SUITE « S »
00	Aucun bit produit
01	Le bit « 0 » est produit
10	Le bit « 1 » est produit
11	Aucun bit produit

On vérifie facilement que les bits de « S' » sont équiprobables, puisque, s'il n'y a aucune corrélation dans la suite « S », la probabilité du paquet « 01 » est la même que celle du paquet « 10 », quel que soit le défaut d'équiprobabilité des « 0 » et des « 1 » de « S ». On voit les limites du procédé : la suite « S » ne doit pas être produite trop rapidement, sinon des corrélations apparaissent. Mais, surtout, la suite « S' » n'est pas engendrée régulièrement : on ne peut prévoir quand un bit sera effectivement créé et le délai d'attente peut être indéfini (même si cela est peu probable). De ce fait, « S' » est une suite arythmique qui ne peut pas être synchronisée avec une horloge distribuant, selon une périodicité fixée, les impulsions nécessaires à l'exécution des opérations d'un circuit séquentiel comme sont les machines à chiffrer. Il est alors nécessaire de forcer, suivant une loi prédéterminée, la production d'un bit, si « S » contient une trop longue suite de bits identiques.

Un tel mécanisme introduit évidemment un biais dans la suite « S' ». C'est pourquoi les dispositifs physiques de génération d'aléa ne sont employés que pour fabriquer des suites assez courtes et peu fréquemment utilisées, comme les clés d'un système de chiffrement.

Photo n° 1. On voit au premier plan Marius GAUBERT et Jean-Pierre VASSEUR, en conversation. Parlent-ils de Myosotis ou de... gastronomie ?

Photo n° 2. On voit de gauche à droite Marc DUMAIRE et Félix RABAUD, et à l'extrême droite le commandant TARIEL.

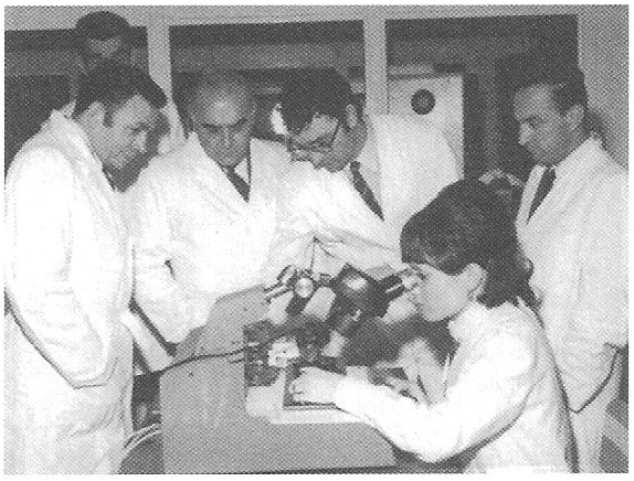


Photo n° 3. On voit André MULLER, debout prononçant un discours, probablement à la fin d'un dîner de l'ARC. On reconnaît également Félix RABAUD (à l'extrême gauche), André BELLON (3e en partant de la droite) et Claude GAUTHIER (à l'extrême droite).

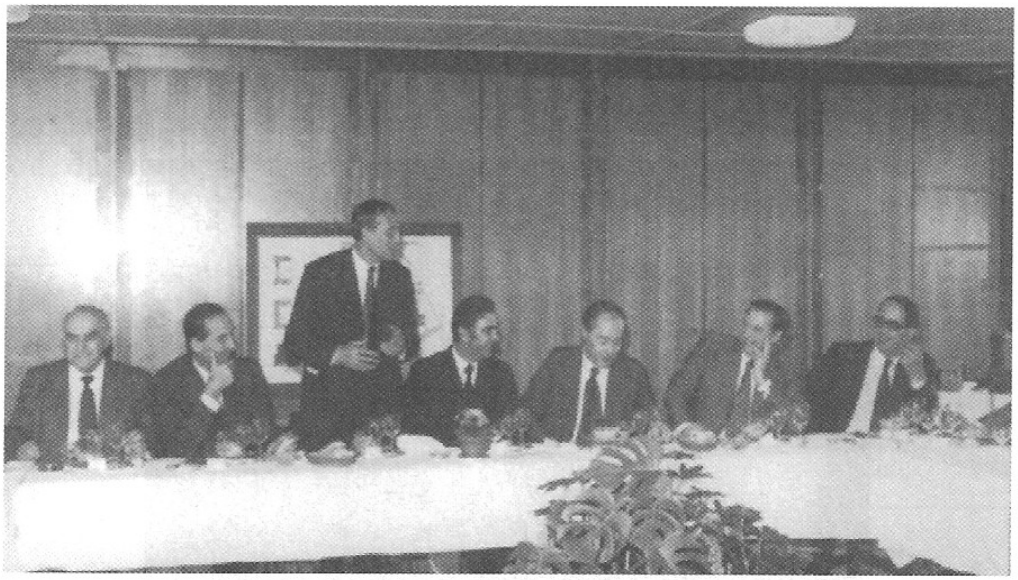


Photo n° 4. Un ensemble de chiffrement télégraphique comprenant, en haut : à gauche le coffret contenant les permutateurs de clé, à droite le bloc de chiffrement Myosotis ; en bas : à gauche un transmetteur automatique, au centre un téléimprimeur, à droite le bloc de commande de Myosotis.

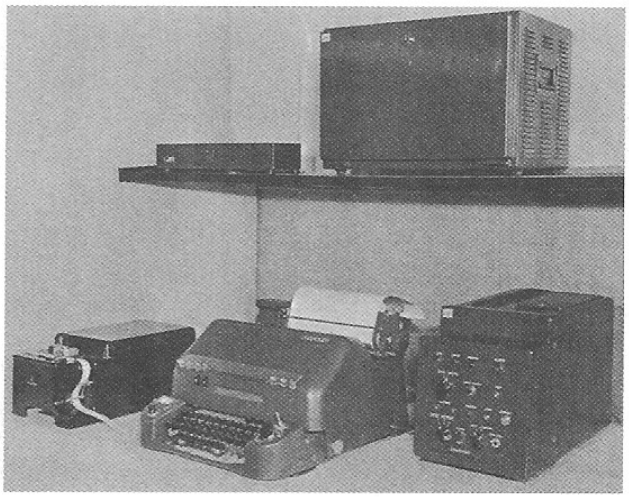


Photo n° 5. Vue interne de Myosotis.

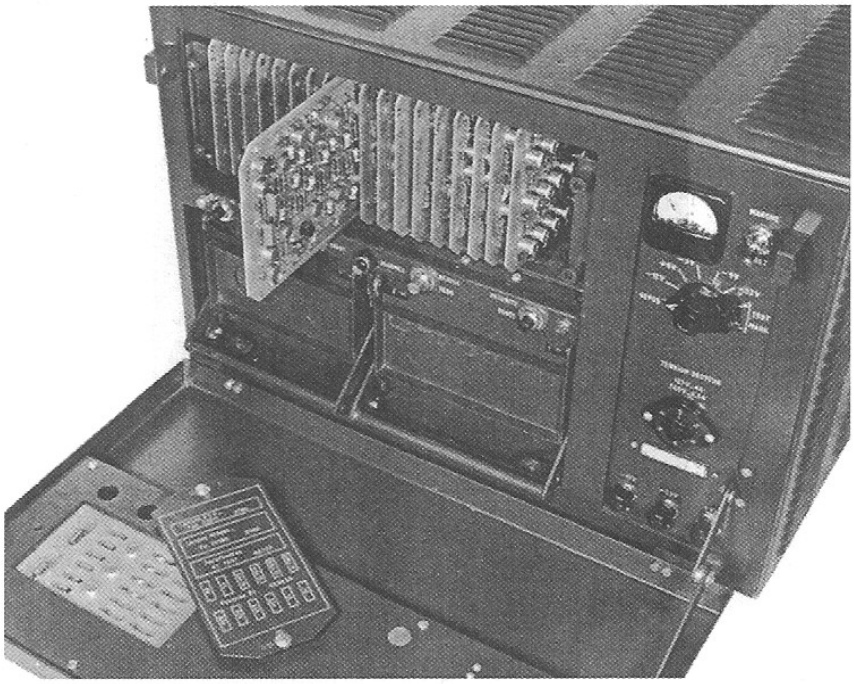


Photo n° 6. Mise à la clé de Myosotis par insertion du panier de permutateurs, préalablement arrangés selon la clé du jour.

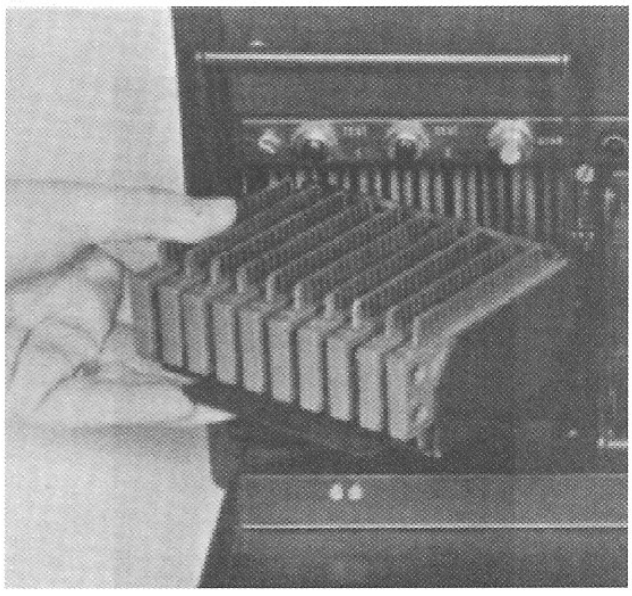


Photo n° 7. Le bloc de télécommande de Myosotis où sont déportées les principales fonctions d'exploitation.

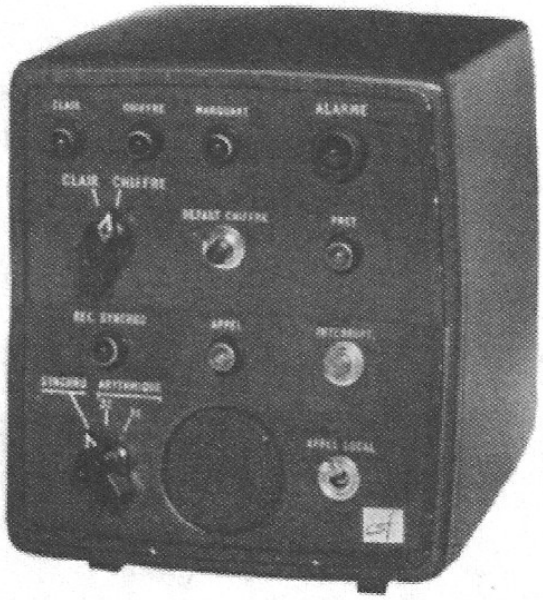
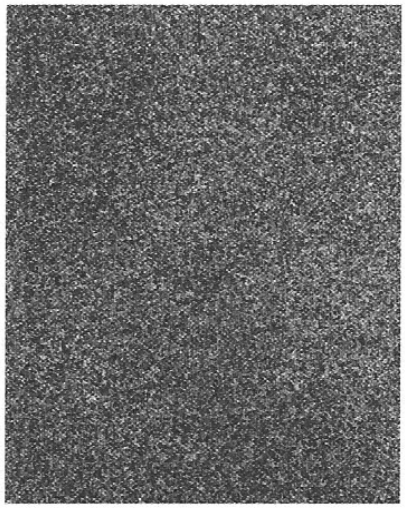


Photo n° 8. Cette photo est l'image d'une page de fac-similé chiffrée par Myosotis. Comme il s'agit d'une page blanche, le crypto est directement la sortie de Myosotis. Cela donne une représentation visuelle de l'aléa produit par Myosotis, sous forme de points blancs ou noirs, selon que le bit de sortie vaut 0 ou 1.



Achevé d'imprimer
sur les presses de l'E.I.A.T. Château-Chinon
2003-10035