LA CRYPTOGRAPHIE EN QUESTION

Par Alexandre PUKALL 1998

email : alexandermail@hotmail.com

L'étude de la science des écritures secrètes ou cryptographie ne se limite pas à la connaissance de la technique du Chiffre, c'est à dire des systèmes pour crypter des données . Elle comprend aussi l'analyse des systèmes de chiffrement du point de vue de leur attaque, c'est-à-dire la connaissance de la théorie de leur décryptement (ou " cassage " du Chiffre) qui permet de retrouver les données de façon illégale sans connaître la clé de décryptement.

Ainsi on sera pleinement en mesure d'évaluer la sûreté cryptographique d'un système et, le cas échéant, d'éviter ou pallier les risques provoqués inévitablement par les accidents, fautes ou erreurs de chiffrement.

C'est souvent, en effet, des erreurs de chiffrement qui ont permis durant l'Histoire, de casser les systèmes de chiffrement des forces ennemies.

S'il existe des principes rigoureux et des règles absolues en Chiffre, il n'en est pas de même en Décryptement et l'on a souvent pu dire dans le passé que le Décryptement était un art.

Aujourd'hui, il tend à devenir plus scientifique, grâce à l'informatique, mais reste cependant essentiellement fonction de la personnalité de l'analyste ou cryptologue.

LES ORIGINES ET LE DEVELOPPEMENT DU DECRYPTEMENT

Les Ecritures secrètes et plus particulièrement le " Chiffre " semblent être nés spontanément dès que, dans un pays, une partie importante de la population a su lire. En tout état de cause, le problème de la conservation du secret des écrits s'impose définitivement avec le développement de l'instruction.

En effet, très rapidement, l'indiscrétion est organisée. On cherche à " intercepter " les dépêches pour les lire. Les curieux installent de véritables écoutes dans les appartements des Césars et des Augustes. C'est sans doute pour cette raison que Jules César introduit le Chiffre...

Parallèlement au souci de conserver le secret des écrits, naît le désir de " percer " le secret des correspondances d'autrui.

La Renaissance qui voit, avec la diffusion de l'instruction, la première période faste du Chiffre, est aussi à l'origine du développement de l'attaque des correspondances chiffrées. Afin de les " élucider ", on intercepte les dépêches chiffrées, on essaie d'en retrouver le texte clair, on fait en définitive de l'analyse cryptographique ou décryptement!

La république de Venise se fait remarquer par la virtuosité de ses décrypteurs. L'un d'eux, Marins, est l'auteur d'un ouvrage traitant du décryptement des dépêches secrètes, Del modo di extrazar le cifre, paru en 1578.

En France, François Viète (1540-1603), rénovateur de l'Algèbre, exerce aussi son savoir et ses talents sur les dépêches chiffrées de la Cour d'Espagne et de Venise au plus grand profit de Henri IV.

Il arriva d'ailleurs à Viète une fâcheuse histoire. En 1545, s'étant vanté imprudemment auprès de courtisans de " lire " les dépêches chiffrées de la Chancellerie d'Espagne, l'ambassadeur de Venise, présent à l'entretien, en fit prévenir Philippe II. Celui-ci ne fit pas moins que d'accuser Viète de sorcellerie et de le faire déférer au tribunal de la Sainte Inquisition. Viète n'échappa au bûcher que sur l'intervention de Rome, convaincue--et pour cause -- du peu de fondement de l'accusation. Viète put ainsi finir ses jours en paix et goûter les honneurs dont Henri IV le comblait.

Rossignol s'est immortalisé moins comme créateur du Chiffre de Louis XIV que comme décrypteur. N'appelle-t-on pas " rossignol " la fameuse clef qui ouvre toutes les portes ? Rossignol était, en effet, un extraordinaire spécialiste des " clefs " (celles du Chiffre bien entendu).

L'on assure que bien peu de dépêches chiffrées à l'époque, lui résistaient. Les débuts de sa carrière remontent à un succès de prestige, obtenu au siège de Réalmont (1626) qui lui valut d'emblée la notoriété.

Au cours de la lutte contre les protestants, le prince de Condé vint à assiéger Réalmont. La ville résistait avec acharnement et l'armée de siège autour de la ville risquait d'être décimée par la maladie. Condé se trouvait donc devant l'alternative soit d'investir la place à bref délai, soit de lever le siège.

Alors qu'il s'apprêtait à abandonner, on captura un homme du parti adverse qui essayait de traverser les lignes. Fouillé, on trouva sur lui un poème si détestable qu'il était logique, eu égard aux circonstances, de lui attribuer une valeur autre que littéraire. On supposa donc rapidement qu'il s'agissait d'un message secret. L'état-major de Condé se mit à l'ouvrage mais désespéra bientôt de le traduire. Alors un des officiers se souvint à propos d'un certain Rossignol, gentilhomme campagnard de la région, passionné de mathématiques et de cryptographie.

Rossignol, âgé de 36 ans, put donner dans la journée la traduction en " clair " du poème. Ce texte, fort révélateur, indiquait que la place manquait de munitions et qu'elle serait dans l'obligation de se rendre si une expédition de secours ne lui était envoyée avec les approvisionnements demandés. Condé, sous la protection d'un drapeau blanc, renvoya sans autre commentaire le message déchiffré aux assiégés de Réalmont. Dès le lendemain matin, la place se rendait.

Ce succès de Rossignol ne devait pas rester sans lendemain. Un an plus tard, il se signalait à l'attention de Richelieu en traduisant des dépêches chiffrées en provenance de La Rochelle. Richelieu, en politique avisé, le mit alors à la tête d'un service spécial de correspondances secrètes. Ses succès en décryptement ne se démentirent pas mais ils

eurent évidemment peu de publicité. Seules les archives du temps font état de sommes versées à lui- même ou à ses collaborateurs pour les services rendus.

Au Grand Siècle, le décryptement était à la mode et certains petits maîtres, jouant les initiés, prétendaient " pénétrer " facilement les textes chiffrés. L'un d'eux, le chevalier de Rohan, s'était même vanté auprès de ses amis de traduire en clair n'importe quel message chiffré sans en posséder la clef. Il fut malheureusement victime de sa vantardise à la suite d'une histoire à la fois rocambolesque et tragique. Pendant la guerre de Hollande (1672-1679), accusé d'avoir livré Quilleboeuf aux Hollandais avec la complicité de son ami La Truaumont, il fut interné à la Bastille en attendant son jugement. L'instruction suivait son cours lorsque Rohan reçut un jour un paquet de chemises. Un message chiffré était inscrit sur la manche de l'une d'elles. Ses amis, convaincus qu'il pourrait lire le message, espéraient le prévenir par ce moyen qu'aucune charge n'existait contre lui, La Truaumont étant mort sans avoir rien dit de leur collusion. Mais Rohan ne put traduire le message chiffré. Pris de peur et s'imaginant qu'on voulait l'informer de la découverte des preuves de la conspiration, il avoua tout à ses juges le lendemain.

Condamné, il paya de sa vie sa suffisance et sa trahison. Le message qui aurait pu le sauver n'avait pourtant été chiffré qu'en substitution simple littérale à représentation unique , procédé perméable et décrypté par les spécialistes de l'époque.

Une autre histoire dont la fin tragique est due à un décryptement réussi est celle de la conspiration du duc d'Argyll, en 1685. Cette conspiration avait pour but de mettre sur le trône d'Ecosse, en lieu et place de Jacques II, frère du défunt Charles II, le duc de Monmouth. fils naturel de ce dernier. Les conjurés crurent prudent d'innover en matière de Chiffre et utilisèrent, pour correspondre entre eux, un procédé de leur invention. Les messages secrets envoyés en Ecosse, interceptés, se composaient apparemment d'une suite incohérente de mots. Mais on s'aperçut vite qu'il s'agissait d'une transposition (ou anagramme) portant sur des mots entiers. Les messages, mis sous une forme plus cohérente, contenaient encore quelques mots sans signification que le sens général des phrases rétablies permettait cependant de supposer comme devant être des noms propres.

Grâce au contexte, il fut relativement facile de rétablir ces noms propres. Les dépêches étant décryptées, le roi Jacques II put prendre des mesures en conséquence.

Le débarquement qui eut lieu en mai 1685 échoua et les têtes des ducs d'Argyll et de Monmouth roulèrent sous la hache du bourreau.

Au XVIII° siècle, le décryptement est en " veilleuse " et Voltaire dans l'article " Postes " de son Dictionnaire philosophique (1764) peut écrire:

" Ceux qui se vantent de déchiffrer une lettre sans être instruits des affaires qu'on y traite et sans avoir de secours préliminaires sont de plus grands charlatans que ceux qui se vanteraient d'entendre une langue qu'ils n'ont point apprise. "

Sous le Directoire, l'état-major français rétablit le " clair " de la correspondance chiffrée saisie en janvier 1796 dans les fourgons du général autrichien Klinglin. Cette correspondance, chiffrée en Jules César, permit d'établir la trahison du général Charles Pichegru, commandant en chef de l'armée française du Rhin.

Au XIXe siècle l'impulsion est donnée par des écrivains. Qui ne se souvient d'avoir lu Le scarabée d'or d'Edgard Poe (1809-1849) ? Dans cette nouvelle, l'analyse du message chiffré du capitaine Kidd est un véritable modèle de décryptement d'une substitution simple. Si la méthode était connue, Edgard Poe eut du moins le grand mérite de la

vulgariser. Il ne s'en tint pas là. Par la voie de la presse, il lança un défi à ses lecteurs, s'engageant à rétablir en " clair " n'importe quel message chiffré en langue anglaise, française, espagnole, italienne, allemande, latine ou grecque. Nous ne savons pas si les envois furent nombreux mais la légende veut qu'il décrypta tous les messages qui lui furent adressés, sauf un. Encore aurait-il réussi à prouver, pour ce dernier, que ce n'était qu'un assemblage de lettres quelconques n'ayant aucun sens plausible en langage " clair " !

Honoré de Balzac (1799-1850) soumet à la sagacité de ses lecteurs deux textes chiffrés. Le premier se trouve dans l'Histoire des treize, le second dans la Physiologie du mariage. Pour ce dernier, le commandant Bazeries a prouvé qu'il s'agissait d'une mystification. Mais sa démonstration reste sujette à caution pour certains. Quoi qu'il en soit, ce texte n'a jamais été décrypté.

Plus connus sont les exemples d'écritures chiffrées donnés par Jules Verne (1828-1905) dans la Jangada, Mathias Sandorf et Voyages au centre de la terre. Ces exemples étaient d'ailleurs techniquement plus évolués que ceux de Poe et de Balzac.

Sous l'impulsion donnée par les romanciers, dès la seconde partie du siècle, les ouvrages techniques abondent. En 1865, paraissent à Berlin les travaux du major de l'armée prussienne Kasiski. On y trouve, en particulier, l'exposé de la première méthode rationnelle de décryptement des messages chiffrés au moyen du " carré de Vigenère ". C'est en 1883 que paraît à Paris un document fondamental, La cryptographie militaire, par Kerckoffs.

Dans cet ouvrage, l'auteur complète les travaux de l'Allemand Kasiski et expose un nouveau procédé de décryptement des " systèmes de substitution à base variable ". En 1805, paraissent dans la Revue maritime et coloniale les articles du capitaine d'artillerie breveté Josse. En 1888 et 1893, sont publiés les travaux du marquis de Viaris. De 1893 à 1896, paraît en librairie le Traité de la cryptographie par le capitaine d'artillerie Valerio. Dans cet ouvrage, l'auteur a essayé d'établir les lois rationnelles du décryptement en étudiant la fréquence des bigrammes et des trigrammes (couples de 2 ou 3 lettres) en français, anglais, italien, espagnol et allemand. De 1896 à 1901, le commandant Bazeries publie des études relatives au décryptement de nombreux textes chiffrés historiques. On lui doit en particulier l'introduction de la notion du " mot probable " dans les travaux de décryptement (le fait de se douter de la présence d'un mot dans le texte crypté permet d'attaquer ce dernier plus facilement). Sa maîtrise en tant que décrypteur fut particulièrement mise en relief lors du complot royaliste de 1890 (affaire Déroulède) et surtout à l'occasion de l'affaire Dreyfus (1894).

Il est remarquable d'ailleurs qu'à partir de la seconde moitié du XIXe siècle jusqu'à nos jours la cryptographie contribue à faire " l'Histoire " ! Mais elle n'a pas plus d'éclat pour cela, bien au contraire ! Un voile discret est jeté sur les services qu'elle rend. Et pourtant tous les pays mènent dans ce domaine une lutte sournoise et farouche, lutte qui devient particulièrement intense et dramatique lorsque les adversaires s'affrontent les armes à la main.

La guerre de Sécession aux Etats-Unis (18-60-1865) est l'occasion d'un des premiers duels notables Chiffre contre Décryptement. Les nordistes utilisent le système Stager présentant quelque analogie avec la méthode employée lors de la conspiration du duc d'Argyll.

Les sudistes se servent d'un système à base de signes et de symboles pour leurs services de renseignements et du " carré de Vigenère " pour leurs télégrammes militaires. Ils disposent, surtout, d'un service d'espionnage excellent et d'une cavalerie spécialisée dans les raids sur les arrières. Cette dernière pratique les " écoutes " en interceptant les

voies télégraphiques de l'adversaire. Mais les spécialistes sudistes ne surent pas profiter de ces renseignements et décrypter les messages chiffrés des nordistes. Ceux-ci, au contraire, excellaient dans le décryptement des communications secrètes des confédérés et ce fait ne fut pas sans contribuer à leur victoire finale.

Pendant la guerre franco-allemande de 1870-1871 les Allemands utilisent le système Gronsfeld dont ils essaient de corriger la faiblesse interne par de fréquents changements de clefs. Les rares messages interceptés furent décryptés par les Français mais les renseignements qu'ils contenaient n'eurent malheureusement qu'une importance locale.

Après 1900, l'usage de la télégraphie sans fil (radio-télégraphie) donne à l'interception et au décryptement un développement sans précédent.

En effet, ce nouveau moyen de transmission, indiscret par sa nature même, livre directement le texte des messages. S'ils sont chiffrés, les rectifications d'erreurs de transmission ou de chiffrement et les bavardages d'opérateurs sont des sources précieuses de renseignements pour les cryptologues. La Grande Guerre devait d'ailleurs illustrer abondamment le grave danger des interceptions. Les rectifications, les répétitions et les conversations téléphoniques ou par radio entre exploitants permirent aux analystes de l'équipe Cartier de s'en donner à coeur joie.

Pendant toute la guerre, les messages allemands interceptés furent le plus souvent décryptés malgré les modifications apportées par les Allemands à leurs systèmes de chiffrement militaires et diplomatiques. Par ses résultats remarquables l'équipe française provoqua l'admiration sans restriction des Alliés. Tous ses membres seraient à citer.

Certains ont leur nom attaché à des ouvrages de Cryptographie. C'est d'abord Cartier, le chef, de qui le général Mordacq a pu écrire " qu'il fut plus utile à notre pays qu'un corps d'armée ". C'est aussi Givierge, auteur d'un traité qui fait toujours autorité.

D'autres, moins connus, ont été cependant les chevilles ouvrières de l'équipe, tel Painvin, qui décrypta, entre autres, un procédé allemand très complexe dit ADFGX et permit ainsi de rétablir le texte clair d'un message d'importance capitale pour la seconde bataille de la Marne (1918), nommé par certains le " Radiogramme de la Victoire ".

Mais les français ne sont pas les seuls à s'être fait remarquer dans l'histoire du décryptement.

C'est aux Allemands que l'on doit une des plus originales et habiles tentatives de déjouer les interceptions et même les analyses des cryptologues.

Au début de la première guerre mondiale, pour correspondre avec le général von Lettow-Vorbeck, isolé en Afrique-Orientale, le Haut Commandement allemand ne disposait que de l'ancien chiffre d'avant-guerre. Méfiant à juste titre, mais ne pouvant faire parvenir de nouveaux codes au général, les spécialistes allemands imaginèrent un stratagème des plus ingénieux. Leurs messages chiffrés, traduits en morse, furent enregistrés sur disques de phonographe tournant à vitesse normale et émis par radio en faisant tourner les disques enregistrés à une vitesse cinq ou six fois plus grande. Tous les soirs la station de Nauen émettait ainsi, à très grande vitesse, des séries de signaux. Après les avoir étudiés les spécialistes avaient conclu qu'il devait s'agir d'une méthode nouvelle de contrôle technique d'émission.

Or, un officier anglais eut par hasard l'idée d'enregistrer ces signaux sur un disque et de faire passer l'enregistrement à vitesse réduite. Les signaux incompréhensibles devinrent alors des longues et des brèves de l'alphabet morse. Le " pot aux roses " était découvert et l'astuce allemande déjouée.

Plus tard, la victoire de Tannenberg est due, en grande partie, à la connaissance par les Allemands du Chiffre russe. Au courant des ordres donnés par le Haut Commandement russe, Hindenburg put manoeuvrer à son aise et non seulement infliger aux russes une cuisante défaite mais aussi éviter l'invasion de la Prusse.

Une heureuse opération des Russes devait d'ailleurs compenser, en partie seulement, le désastre de Tannenberg.

Au cours d'une sortie dans la Baltique, le croiseur léger allemand Magdebourg échoua et fut surpris par la flotte russe. Le commandant du navire allemand, sans illusion sur le combat qui allait s'engager, voulut empêcher le code secret en sa possession de tomber entre les mains des Russes. Il chargea donc un officier marinier de l'immerger aussi loin que possible du croiseur.

Dans toutes les marines du monde, les codes secrets sont reliés en plomb afin d'éviter, en cas de naufrage, la remontée en surface des documents. L'officier marinier chargé de l'opération se noya avant d'avoir pu la mener à bien et son corps fut ramené à la côte et trouvé par les Russes.

Le malheureux serrait encore dans ses bras les couvertures plombées. Le commandement russe, ayant toutes les raisons de supposer que les codes eux-mêmes ne devaient pas se trouver loin, fit entreprendre des recherches. Des marins plongèrent et eurent la bonne fortune de ramener, à peine endommagé, le code naval allemand au complet. Pendant deux ans environ, jusqu'à la bataille du Jutland (1916), les Alliés purent déchiffrer la majeure partie des radiogrammes maritimes de l'ennemi, malgré de fréquents changements de clefs.

Après 1918, la Cryptographie et surtout le Décryptement jouissent d'un regain d'intérêt. Les articles du général Cartier et du colonel Givierge, grâce à l'audience des revues dans lesquelles ils paraissent, l'édition d'ouvrages fort bien présentés et quelquefois romancés introduisent à nouveau les notions de décryptement dans le grand public. Mais en 1939, à la veille de la seconde guerre mondiale, les enseignements de la Grande Guerre en matière de décryptement étaient déjà oubliés, du moins en France.

Un nouvel essor, considérable, du décryptement va pourtant se produire au cours du conflit chez tous les belligérants. Des équipes de spécialistes sont constituées dont la tâche consiste à faire l'analyse des procédés et systèmes de chiffrement ennemis et à tenter de les décrypter. L'effort consenti est d'une ampleur sans précédent. La nombreuse littérature, tant technique que romancée, parue depuis 1945 sur le sujet en est la preuve. Mais il est encore mieux de rapporter l'opinion autorisée de Sir Winston Churchill qui a pu dire que " trois facteurs ont permis de gagner la bataille d'Angleterre: la Home Fleet, la Royal Navy et la Cryptographie " (il parlait bien entendu du décryptage des machines allemandes ENIGMA).

Les succès obtenus dans l'attaque des correspondances secrètes pendant le conflit ont frappé les imaginations et, aujourd'hui, l'indiscrétion, élevée à la hauteur d'une institution, prend les formes les plus diverses. On intercepte les communications de toutes natures. On installe des microphones et des magnétophones pour capter les conversations. On utilise des tables d'écoutes pour entendre les communications téléphoniques. Des postes radio à forte puissance et gamme d'onde étendue surveillent les émissions radio. Même si les conversations confidentielles ont lieu en langage convenu, si les communications téléphoniques et les télégrammes sont chiffrés, les écoutes continuent. Les indiscrétions d'opérateur, les accidents de chiffrement, les erreurs et fautes des chiffreurs permettent aux décrypteurs d'obtenir des résultats favorables.

Dans les années 50, apparu le triage mécanique des répétitions, le calcul automatique des relations numériques liant entre eux les éléments des cryptogrammes interceptés évitant les travaux longs et fastidieux de naguère tout en éliminant les sources d'erreurs.

Aujourd'hui, les ordinateurs facilitent encore ces travaux préliminaires. Le décryptement s'oriente vers l'utilisation de méthodes plus scientifiques que dans le passé. Mais l'analyse des cryptogrammes à partir de méthodes scientifiques (statistiques en particulier) exige un nombre considérable de cryptogrammes, un équipement d'ordinateurs et du personnel capable d'en établir le logiciel et d'effectuer la programmation.

INTERNET ET LES RESEAUX MONDIAUX

Le développement d'Internet en fait partie intégrante: des milliards de caractères sont échangés chaque jour.

D'un côté cela noie les documents chiffrés parmi tous les autres mais d'un autre cela permet aux gouvernements avec l'aide de super-calculateurs d'avoir assez de documents chiffrés pour tenter de casser le système s'ils l'estime nécessaire.

La tâche est d'autant plus aisée que malgré ce que l'on croît, Internet est très centralisé ! En effet, en France (comme dans tous les pays), chaque message envoyé par Internet même s'il est destiné à quelqu'un habitant la même ville que vous, passe par le noeud de Transit International de Paris, qui redistribue le message vers les noeuds informatiques étrangers ou les renvoie sur la ville destinatrice.

Ainsi un centre d'écoute implanté à Paris permettrait d'intercepter tous les messages échangés en France, sortant de France ou y entrant !

Le seul cas où les messages ne passent pas par Paris, est lorsque le message est destiné à un utilisateur hébergé par le même fournisseur d'accès que l'émetteur et si ce fournisseur d'accès est situé dans la même ville.

C'est le cas pour les petits fournisseurs d'accès locaux. Dans ce cas le message reste dans l'ordinateur du fournisseur d'accès et est distribué lorsque le destinataire se connecte.

Dans les autres cas, où le fournisseur d'accès a plusieurs points d'accès (Wanadoo, AOL, Compuserve, Infonie, HOL ...) le message passe par Paris.

Un tel centre d'interception existe-t'il ? Personne ne le sait. Aux Etats-Unis la probabilité qu'un tel centre existe est très très forte : L'Etat Fédéral a demandé en 1997 à tous les opérateurs téléphoniques d'intégrer d'ici à 2002 dans leurs centraux téléphoniques un système permettant d'écouter simultanément 1% des lignes téléphoniques du pays !

Si on estime le nombre de lignes à 260 millions cela fait 2,6 millions d'écoutes téléphoniques possibles à la fois !

Ceci ne concerne que les écoutes à la source, c'est-à-dire directement sur la prise téléphonique chez l'habitant (que des données ou de la voix circule sur cette ligne) mais à cela s'ajoute le fait d'écouter les noeuds de transits internationaux : En effet, Internet

est né du réseau américain Arpanet, cela explique que des communications par Internet du Japon vers la France peuvent passer par les USA pour arriver en France.

Ainsi les Etats-Unis peuvent aussi intercepter des communications Internet de pays étrangers !

En France, il est possible qu'un tel centre d'interception existe mais aucune preuve n'existe, tout en bien sûr secret.

Pour ma part, je pense que oui en ce qui concerne le centre d'écoute du noeud de Transit. En effet, la loi limitant les écoutes téléphoniques ne s'applique pas sur le noeud de Transit, car ce n'est pas une écoute d'un individu particulier mais une écoute globale faite par des ordinateurs sur les informations qui y circulent à la recherche d'informations illégales (tri sur des mots clefs : " marchandises arrive demain ...", analyse d'images ...)

Ce qu'il faut savoir c'est que la technique permet de le faire aussi bien pour les communications Internet que les lignes vocales ou que les téléphones mobiles GSM (Group Special Mobile).

Des valises d'interceptions de téléphones GSM existent et valent 40000 dollars. Elles permettent d'enregistrer simultanément 1000 conversations de téléphones GSM (voix, données ...).

Au 5 avril 1998, une documentation de ces valises d'interceptions peut se trouver sur le site :

http://www.mygale.org/05/pccom.gsm.htm

Y sera-t'elle encore quand vous lirez cet article ? Personne ne peut le dire, les sites Internet apparaissant et disparaissant très rapidement ! C'est pour cela que je l'intègre à cet article : si vous lisez cet article sur support informatique, vous devriez trouver non loin de loin un fichier HTML du nom de GSM.HTM et un fichier image représentant la valise d'interception du nom de CELLULAR.GIF

Ce qui est sûr c'est qu'Internet n'est pas anonyme alors restez sages ! Ne tentez pas le diable même pour essayer : ne tentez pas de récupérer des images pédophiles et de les diffuser " pour voir ". Chaque fois que vous émettez un message ou un fichier sur Internet, votre adresse IP (Internet Protocol) est émise en même temps, non pas par votre ordinateur, mais par votre fournisseur d'accès.

Cette adresse IP est utilisée pour que le serveur destinataire puisse vous envoyer automatiquement une réponse, réponse que vous ne voyez pas forcément, et qui correspond souvent à un accusé de réception (ACK): message ou fichier bien reçu.

Vous ne pouvez pas enlever cette adresse IP vous-même (d'ailleurs sans adresse IP vous ne pourriez pas vous connecter à un site Web puisque le site ne saurait pas où envoyer les pages Web demandées !).

Ainsi si vous transmettez des fichiers ou images illégales et que ces fichiers sont interceptés, il suffit de regarder l'adresse IP pour savoir de quel fournisseur d'accès provient le fichier.

Ces adresses IP ne sont pas fixes : lorsque vous vous connectez le lundi, vous aurez peut-être l'adresse IP: 195.242.98.234

Lors d'une nouvelle connexion une heure plus tard vous en aurez un autre : 195.242.64.150 etc...

Ces adresses appartiennent à une plage d'adresse que le fournisseur d'accès a le droit d'utiliser.

Cependant, à chaque connexion à votre fournisseur d'accès, votre nom de login (nom de connexion) est enregistré dans un fichier avec l'adresse IP dynamique correspondante.

Ainsi un fichier intercepté contenant l'adresse IP (il contient aussi le jour, l'heure, les minutes et les secondes de l'envoi du fichier) permet de connaître le fournisseur d'accès.

Il suffit ensuite aux forces de police de demander à ce fournisseur d'accès de consulter son fichier historique à l'endroit correspondant au jour, heure, minutes, secondes en question puis de comparer à qui appartenait l'adresse IP en question pour retrouver la personne physique qui a envoyé le fichier !

C'est d'ailleurs comme cela que se sont fait prendre bon nombre de pirates informatiques qui essayaient de pénétrer dans les services informatiques du ministère de la Défense, ou des personnes ayant échangées des images pédophiles sur Internet.

Et ne croyez pas que le fait de se connecter par Internet sans abonnement (par France Explorer, Infonie Direct ...) préserve votre anonymat.

Ces systèmes vous permettent de vous connecter à Internet en passant par un numéro spécial du type : 08 36 68 XX XX) où vous payez plus cher (1,25 F la minute) mais sans abonnement.

Au début on vous demande votre adresse mais même si vous donnez une fausse adresse et un faux nom, vous ne restez pas anonyme.

En effet, depuis octobre 1997, le numéro de téléphone appelant apparaît chez le destinataire. Ces numéros sont enregistrés dans le fichier historique des fournisseurs d'accès sans abonnement avec l'adresse IP du moment et les dates, heures ...

Normalement vous pouvez demander à France Télécom que votre numéro n'apparaisse pas chez le correspondant. C'est gratuit et cela marche sauf pour les destinataires spéciaux : SAMU, POMPIERS, certains services de police et les fournisseurs d'accès direct Internet !

Vous n'êtes donc pas anonyme sur Internet, alors ne tentez pas le diable ! Même le fait de crypter vos fichiers, n'empêchera pas une descente de police chez vous pour vérifier que vous ne faites rien d'illégal !

LE CHIFFREMENT MODERNE

Pour en revenir au chiffrement proprement dit, à partir des années 70 le cryptage s'est radicalement transformé. Auparavant existaient les systèmes manuels jusqu'en 1920

puis apparurent les systèmes électro-mécaniques (machines ENIGMA, SIGABA ...) puis apparurent après la deuxième guerre les machines électroniques.

Enfin après 1970, ce sont les systèmes informatiques qui prirent le relai. Les systèmes devenaient des milliers de fois plus performants que les machines électroniques car l'ordinateur permettait des possibilités nouvelles et illimitées. Grâce à lui on peut créer des systèmes de chiffrement ultra-performants très simplement sans devoir souder des tas de composants sur des cartes électroniques.

Le cryptage des données autrefois réservé aux militaires est apparu dans le grand public grâce à l'ordinateur et les systèmes actuels peuvent résister même aux attaques des gouvernements les plus puissants !

DESCRIPTION DE SYSTEMES DE CHIFFREMENT MANUELS

LE CHIFFREMENT JULES CESAR

Le chiffre de César est une substitution monoalphabétique à alphabet régulier. Chaque lettre est décalée d'une position allant de 1 à 25 (exemple avec un décalage de 1: ABCD devient BCDE).

Jules César, pendant les guerres de Gaule, correspondait avec ses partisans restés à Rome au moyen de messages chiffrés à l'aide d'un décalage de petite amplitude (3 lettres) de l'alphabet. Malgré la simplicité d'une telle méthode (il suffit d'essayer les 25 décalages possibles du texte pour casser le système), il semble que ce chiffre n'ait jamais été décrypté à l'époque. Il faut néanmoins noter que César lui-même écrit qu'il vaut mieux utiliser un messager sûr et fidèle et qu'il abandonne ce système jugé trop dangereux dès l'instant où son principal correspondant, Cicéron, change d'idées politiques et par conséquent de camp.

Les chiffres à alphabet chiffrant régulier sont pourtant bien antérieur aux Romains. Ils sont déjà utilisés par les indiens et les hébreux, tels l'Albam ou l'Atbash qui sont des chiffres hébraïques. L'Albam est un chiffre décalé et l'Atbash un chiffre inversé.

Il faut dire qu'à cette époque l'utilisation du chiffre n'est pas systématique et qu'en général, seuls les noms propres, les actes vils ou sacrilèges sont chiffrés. Un exemple classique se trouve dans la Bible : Jérémie chapitre 25 verset 26 : " ... et le roi de Shéshak boira après eux ... ". Le mot Shéshak est écrit en Atbash et donne " Babel ". On retrouve le même cryptogramme au chapitre 51 verset 41.

Notons encore, pour la petite histoire, qu'en juillet 1862, le général Albert S. Johnston, que l'on dit pourtant excellent officier, convint avec son homologue Pierre Beauregard, d'une substitution de type Jules César pour l'usage militaire ! et qu'en 1915, les russes remplacèrent leur code par un César, seul chiffre que les moujiks, à demi illettrés, pouvaient utiliser. Ce fut la période la plus faste des services de décryptement autrichien et allemand, qui pouvaient lire presque à vue les communications adverses !!

Le chiffre César est très simple à mettre en oeuvre : On choisit le décalage et on l'applique sur chaque lettre. Si on dépasse Z, on repasse à A :

Voici un exemple décalé de 2. Pour le décoder il faut soustraire deux lettres à chaque lettre. Si on passe en dessous de la lettre A on repasse à Z (c'est ce que l'on appelle une soustraction modulo 26).

RQKPVGB N CTVKNNGTKG UWT NC XKNNG

Le fait de laisser les espaces donne un avantage à un éventuel décrypteur. Souvent on groupe le texte codé selon les normes télégraphiques postales, par groupe de cinq lettres en omettant les espaces :

RQKPV GBNCT VKNNG TKGUW TNCXK NNG

Dans ce cas celui qui doit décoder le message devra aussi recomposer les espaces de lui-même. Pour éviter cela on peut ajouter un symbole qui représente l'espace et qui entrera dans le processus de décalage comme une lettre après la lettre Z. On peut prendre par exemple le ?.

Ce qui donnerait :

RQKPVGABNBCTVKNNGTKGBUWTBNCBXKNNE

et en groupes de cinq lettres :

RQKPV GABNB CTVKN NGTKG BUWTB NCBXK NNE

Le point d'interrogation (?) n'apparait pas car aucune lettre du texte clair décalé de 2 ne tombe sur lui (position 27).

Par contre si le texte clair était :

BONJOUR Y AU REVOIR Z

On aurait :

DQPLQWTB?BCWBTGXQKTBA

et en groupes de 5 :

DQPLQ WTB?B CWBTG XQKTB A

LE CHIFFREMENT MONOALPHABETIQUE A ALPHABET DESORDONNE

Le chiffrement César est particulièrement simple à décrypter, du fait que l'identification d'un seul couple lettre claire, lettre chiffrée révèle entièrement la substitution. Si on sait que A donne C, on sait que le décalage est de 2 pour toutes les autres lettres du texte.

Une façon d'améliorer le chiffrement César consiste à remplacer l'alphabet standard par un alphabet désordonné.

Dans le Chiffre César on part de l'alphabet normal (ABCDEFGHIJKLMNOPQRSTUVWXYZ) et on décale les lettres à l'intérieur de celui-ci.

Si on prend comme alphabet initial celui-ci :

KLAMBNUCGOVDHPWZEIQSXFJRTY

et si on prend un décalage de 7 on aura :

A donne C, B donne G, C donne O ...

Ainsi on aura l'alphabet final :

CGOVDHPWZEIQSXFJRTYKLAMBNU

Ce système utilise deux clés : la première est l'alphabet désordonnée initial (KLAMBNU ....), la deuxième est le décalage de 7 lettres.

Cependant on remarque que le système de décalage n'apporte rien de plus que si on ne prenait que le premier alphabet désordonné. En effet, il ne fait que créer un autre alphabet désordonné mais n'apporte pas plus de sécurité.

C'est pour cela que tous les systèmes basés sur ce principe et utilisés dans le passé, n'utilisaient pas de décalage par dessus le premier alphabet désordonné.

En prenant l'alphabet désordonné suivant on peut coder un texte :

ABCDEFGHIJKLMNOPQRSTUVWXYZ donne :

KLAMBNUCGOVDHPWZEIQSXFJRTY

Donc le texte BONJOUR donne LWPOXI

Si on trouve que B donne L, cela ne permet pas de trouver à quoi correspondent les autres lettres, à l'inverse du système César.

Comment casser ce système ? Il suffit de faire une analyse statistique sur le texte : En français les lettres les plus fréquentes sont : E S A I N T U R L O . (NB: l'espace est plus fréquent encore que la lettre E).

Ainsi en comptant le nombre de fois qu'une lettre apparaît dans le texte chiffré, on peut effectuer une attaque statistique. On classe ensuite les lettres par fréquence décroissante.

La lettre la plus fréquente sera le E, ensuite on aura le S ...

Si la lettre R apparaît 115 fois dans le texte chiffré, la lettre U 85 fois et la lettre S 63. Alors R sera la lettre claire E, U sera S et S sera A.

En général les fréquences sont correctes pour E, S et A. Pour les autres lettres cela dépend du type de texte clair et de sa longueur. Une fois que l'on a ces trois lettres, on procède par tâtonnements : on fait des tests : avant le E il peut y avoir un L, un D ... (DE, LE ...)

On essaye si chaque lettre trouvée donne un texte possible dans le reste du texte chiffré.

Avec un ordinateur, un programme peut faire les tests automatiquement s'il possède un dictionnaire de mots.

Ce système peut cependant être très utile pour protéger des messages sur un canal pouvant subir des perturbations : par exemple un canal radio.

Si des lettres sont perdues ou abîmées, ce système permet quand même de décoder la fin du message qui n'a pas été touchée. Avec les systèmes informatiques très puissants, si une lettre (même un bit) du texte codé est perdue ou abîmée, tout le texte est indécodable et doit être retransmis.

Les cibistes utilisent de plus en plus la cibie pour se transmettre des messages de type texte par l'intermédiaire de leur ordinateur relié à une interface, elle-même reliée à la cibie (interface de type HAMCOMM). Ces interfaces transmettent les textes en MORSE, en BAUDOT, en FEC ...

Un système de codage du texte qui peut être utilisé même si une lettre est perdue (ce qui arrive souvent en transmission par cibie) est idéal.

Je joins un programme du nom de CRYPTO VADOR (en référence au film " l'Empire Contre-attaque ", où les sondes de l'Empire transmettent leurs informations en " Code Impériale ").

C'est un programme DOS Résident (TSR) pour PC composé de trois parties :

CLE.EXE

CRYPTO.EXE

VADOR.EXE

A noter qu'aucun programme de ce type n'existe à l'heure actuelle pour coder des textes automatiquement par cibie sur PC. D'autres existent mais il faut coder le texte dans un logiciel de codage puis l'importer dans le logiciel d'émission.

CRYPTO VADOR permet de faire du chiffrement en ligne, c'est-à-dire de coder le texte en même temps qu'il est tapé sur le clavier du PC.

CRYPTO.EXE est un programme résident qui transforme les lettres que vous tapez au clavier en lettres codées suivant le principe de substitution monoalphabétique avec alphabet désordonné (exposé ci-dessus).

VADOR.EXE est un programme résident qui transforme les lettres codées reçues en lettres claires.

CLE.EXE est un programme qui permet de créer les alphabets désordonnés à partir d'un mot de passe. CLE.EXE utilise un mot de passe de 10 caractères, ce qui correspond (si on utilise tous les caractères du clavier à 8 bits) à 2 puissance 80 possibilités d'alphabet désordonné. (CLE.EXE utilise l'algorithme PC1 : Pukall Cipher 1 pour créer les alphabets désordonnés à partir du mot de passe).

Une fois l'alphabet créé il est écrit dans les programmes CRYPTO.EXE et VADOR.EXE et est utilisé pour coder les lettres. Tant que vous ne relancez pas CLE.EXE pour créer un autre alphabet, c'est le même qui est utilisé à chaque fois que vous lancez CRYPTO.EXE et VADOR.EXE

Le processus d'utilisation est le suivant :

Lancez CLE.EXE pour créer l'alphabet désordonné

Lancez CRYPTO.EXE

Lancez VADOR.EXE

Une fois lancé CRYPTO.EXE ne peut pas être désinstallé (VADOR.EXE peut être désinstallé en le relançant).

Si vous voulez arrêter ces programmes ou changer l'alphabet désordonné, il faut d'abord rebooter le PC !

Ces programmes ont été testés avec l'interface HAMCOMM pour transmettre du texte codé.

Après le lancement de CRYPTO.EXE et VADOR.EXE rien ne se passe.

Vous devez passer sur le logiciel HAMCOMM (pour DOS) ou un autre programme du même type (PACTERM ...) et passer en mode émission. Appuyez sur la touche ! (sur le clavier français c'est la touche à côté de la touche Shift Droit), chaque lettre que vous allez taper va être codée. Pour arrêter retapez sur !

Pour décoder un texte reçu appuyez sur ALT-H. (avant vous devez avoir retapé sur ! pour arrêter le codage).

Les seules touches qui peuvent être codées sont les touches de A à Z et de 0 à 9 (plus la touche espace) sur le clavier principal. Les touches du pavé numérique ne sont pas codées.

Les deux correspondants doivent bien sûr avoir le même mot de passe pour pouvoir créer les mêmes alphabets désordonnés.

A noter qu'un alphabet désordonné est déjà présent dans CRYPTO.EXE et VADOR.EXE, vous pouvez donc ne pas lancer CLE.EXE et utiliser l'alphabet par défaut.

Autre note importante : les programmes ne doivent pas être utilisés sous Windows 95 ou Windows 3.11 : vous devez quitter le PC en mode MS-DOS pour les utiliser. Les programmes ne fonctionnent pas sous Windows NT.

Le fonctionnement n'est cependant pas garanti, car étant des programmes résidents, ils peuvent planter l'ordinateur.

Vous devez libérer le plus de mémoire conventionnelle possible et éviter de lancer les gestionnaires de mémoire du type QEMM, EMM386.

Des tests ont été faits sur une dizaine d'ordinateurs en MS-DOS 4.1, MS-DOS 5.0 et MS-DOS 6.22 et le programme a l'air de se comporter normalement.

Le fichier CODE.DOC joint contient une série de messages transmis par l'interface HAMCOMM avec CRYPTO VADOR (CODE.DOC contient uniquement les messages reçus et pas les messages émis).

LE CHIFFREMENT POLYALPHABETIQUE (appelé aussi substitution à double clef)

Ce système est apparu en 1587 est utilise en fait plusieurs chiffrement César en même temps.

Une légende s'est créée autour de ce système et celui-ci fut considéré comme le chiffre indécryptable par excellence. En 1917, cinquante ans après que ce système fut cassé, une revue aussi sérieuse que Scientific American le donnait pour impossible à décrypter.

Ce système fut en usage dans les armées françaises (Chiffre de St Cyr), autrichiennes et italiennes (Chiffre de poche) durant la première guerre mondiale, et ce pas toujours au profit de la sécurité des communications.

Comme indiqué ci-dessus ce système mixe en fait plusieurs décalages de type César.

La première lettre du texte est décalée de 9

La deuxième lettre du texte est décalée de 5

La troisième lettre du texte est décalée de 17

La quatrième lettre du texte est décalée de 3

.....

Ceci à partir d'une clé initiale (ci-dessus la clé est 9-5-17-3)

On général on prend un mot ou une phrase pour créer la suite des décalage. On prend A=0, B=1 ... Z=25, ?=26. (on aurait pu prendre A=1, B=2, ... Z=26, ?=27 ça marche aussi)

Si le mot de passe est BRAVO on aura la suite : 01-17-00-21-14

On répète cette suite pour coder le texte clair.

Si le texte clair BONJOUR A VOUS, on transforme ce texte clair en chiffre : (on rajoute le signe ? comme espace et de numéro 26). On y ajoutera la clé modulo 27 (si >26 on repasse à 0)

01-14-13-09-14-20-17-26-00-26-21-14-20-18 on y ajoute la clé:

01-17-00-21-14-01-17-00-21-14-01-17-00-21

=

02-31-13-30-28-21-34-26-21-40-22-31-20-39 si >26 on repasse à 0

=

02-05-13-04-02-21-08-26-21-14-22-05-20-13 ce qui donne :

=

CFNECVI?VOWFUN comme texte codé pour BONJOUR A VOUS avec la clé BRAVO.

Pour trouver le texte clair à partir de CFNEC VI?VO WFUN on soustrait modulo 27 (si < 0 on repasse à 26) avec la clé BRAVO.

Ce système n'est malheureusement pas sûr et peut être cassé en 2 à 3 minutes sur un PC 386 DX 25 pour 100 Kilo-octets de texte. En 5 secondes pour 5000 caractères.

Il existe des logiciels Shareware à la pelle qui utilisent ce système. Par exemple ALTER ou 007. 007 indique que l'on peut utiliser une clé jusqu'à 2048 bits et que par conséquent le système est inviolable. Pour preuve il donne un texte de 150 caractères à essayer de casser.

Il est vrai qu'un seul texte de 150 caractères de pourra pas être cassé. Par contre dans un utilisation réelle, on codera plusieurs textes avec la même clé. Dans ce cas il suffit de 3 à 7 textes de 150 caractères pour casser le système.

Si on ne possède qu'un seul texte il faut qu'il ait une longueur entre 10000 et 15000 caractères (si la clé est de 2048 bits) pour pouvoir le casser rapidement (en une quizaine de secondes).

Laissez tomber ce système de substitution polyalphabétique, il n'est pas sûr !

C'est étonnant de voir encore et encore les mêmes vieux systèmes surgir. Je pense que cela doit être parce que c'est celui que les apprentis programmeurs commencent à étudier !

En effet, comme on mixe simplement plusieurs César ensemble : une fois qu'on connaît la longueur de la clé (ici 5), on dispose le texte codé en colonnes correspondant à la clé : 1er caractère puis en dessous le 6ème puis le 11e puis le 16e ... pour la colonne 1.

Le 2eme puis en dessous le 7e puis le 12e ... pour la colonne 2 ...

Il y a cinq colonnes en tout.

Dans chaque colonne on regarde quel est le caractère le plus fréquent : ce sera l'espace.

Si ce caractère est le T, sachant que T=19 et espace=26, on effectue 19-26= -7 modulo 27 = -7+26 = 19.

La première colonne est décalée de 19.

On effectue la même chose pour les 4 autres colonnes et on trouve les 5 décalages utilisés !

Il faut seulement disposer de 150 à 200 caractères de texte codé pour y arriver.

Pour trouver la longueur de la clé, il suffit de faire une analyse statistique sur les blocs de textes chiffrés. Comme la clé se répète pour coder le texte clair et comme la langue française (comme les autres) est répétitive : LE GARCON ET LE CHIEN : LE se répète deux fois, automatiquement sur 150 à 200 caractères des blocs de textes clairs seront codés par la même partie de la clé. On aura alors des blocs de textes chiffrés identiques. En comptant l'espacement entre ces blocs en en faisant une moyenne, on retrouve la longueur de la clé.

Ce système est donc facilement cassable et pourtant c'est celui qui est utilisé dans bon nombre de logiciels Freeware, Shareware ou Commerciaux (comme Word 6.0 de Microsoft).

LE CHIFFREMENT PAR TRANSPOSITION SIMPLE A COLONNE PLEINE

L'usage de la transposition remonte fort loin dans l'histoire. Les documents les plus sûrs sont ceux qui concerne la scytale des Lacédémoniens, signalée par Plutarque comme utilisée dès l'époque de Licurgue, soit au IX ième siècle avant Jésus-Christ. Elle consiste en un bâton sur lequel on enroulait en hélice un ruban de cuir. Le message était écrit selon les génératrices du cylindre et complété éventuellement de lettres nulles (lettres identiques pour remplir la fin du ruban). Une fois déroulée, cette lanière était portée comme ceinture par le messager. Le texte qui s'y trouvait écrit, transposition du message de départ, pouvait passer pour une invocation aux dieux et déesses pour les rendre favorables au voyage du porteur. Le destinataire possédait évidemment un bâton d'exactement même diamètre.

Durant la première et la Seconde guerre mondiale (au début de celles-ci), l'armée allemande utilisa un système de double transposition (une transposition répétée deux fois) pour ses communications au niveau des petites unités.

Le chiffrement par transposition simple à colonne pleine appelé aussi transposition simple à rectangle complet consiste à écrire le texte en colonnes puis à le relever dans l'ordre de la clé.

On choisit un mot clé :

VICTOIRE et on le transforme en chiffre par le procédé suivant :

On procède de gauche à droite et sous chaque lettre on inscrit sa position par rapport à sa place dans l'alphabet en ordre croissant.

C'est assez difficile à décrire mais plus facile à comprendre comme ceci :

Dans le mot VICTOIRE, la première lettre présente dans l'ordre de l'alphabet est le C. On écrit 1 sous le C.

La deuxième est le E. On écrit 2 sous le E.

La troisième est le I. Or, il y a deux I, on écrit 3 sous le premier à gauche et 4 sous le deuxième.

La quatrième est le O, on écrit 5 dessous.

La 5 ème est le R, on écrit 6 dessous.

La 6 ème est le T, on écrit 7 dessous.

La 7 ème est le V, on écrit 8 dessous.

On a donc :

V-I-C-T-O-I-R-E

8-3-1-7-5-4-6-2

On écrit ensuite le texte en 8 colonnes (longueur de la clé). On utilise le ? pour l'espace. On complète la fin du texte par des espaces. Le texte initial est : J?ORDONNE?LE?LANCEMENT?DE?TOUS?LES?MISSILES?NUCLEAIRES

1-2-3-4-5-6-7-8

J-?-O-R-D-O-N-N

E-?-L-E-?-L-A-N

C-E-M-E-N-T-?-D

E-?-T-O-U-S-?-L

E-S-?-M-I-S-S-I

L-E-S-?-N-U-C-L

E-A-I-R-E-S-?-?

On relève ensuite les colonnes dans l'ordre de la clé : 8-3-1-7-5-4-6-2

Colonne 8 donne NNDLIL?

Colonne 3 donne OLMT?SI

Colonne 1 donne JECEELE

Colonne 7 donne NA??SC?

Colonne 5 donne D?NUINE

Colonne 4 donne REEOM?R

Colonne 6 donne OLTSSUS

Colonne 2 donne ??E?SEA

Donne le texte crypté :

NNDLIL?OLMT?SIJECEELENA??SC?D?NUINEREEOM?ROLTSSUS??E?SEA

et en groupes de 5 lettres :

NNDLI L?OLM T?SIJ ECEEL ENA?? SC?D? NUINE REEOM ?ROLT SSUS? ?E?SE A

Pour décoder il suffit de faire l'inverse. On calcule les chiffres de la clé d'après la clé on obtient : 8-3-1-7-5-4-6-2

On compte le nombre de caractères du texte codé que l'on vient de recevoir. Ici 56. On effectue 56 divisé par 8 (8 = taille de la clé) ce qui donne 7. On sait donc que les lignes sont au nombre de 7.

On va donc remplir les colonnes avec 7 lettres chacune.

On prend les 7 premières lettres du texte codés : NNDLIL? que l'on écrit dans la colonne 8.

Colonne 8

N

N

D

L

I

L

?

On fait de même avec la suite OLMT?SI dans la colonne 3 ...

A la fin on obtient le texte clair initial.

Pour décrypter ce système (le "casser") , c'est-à-dire trouver le texte clair sans connaître la clé initiale. On procède par essais successifs.

La première chose à faire est de trouver la longueur de la clé.

Pour cela on compte la longueur du texte crypté (ici 56) et on divise par toutes les longueurs de clés possibles qui donnent un nombre entier. On part sur le principe que la clé sera inférieure ou égale à 10 caractères dans une premier temps et on essaye ensuite les longueurs plus grandes.

Pour 10 caractères on essaye :

56 : 10 = 5.6

56 : 9 = 6.2

56 : 8 = 7 <--

56 : 7 = 8 <--

56 : 6 = 9.3

56 : 5 = 11.2

56 : 4 = 14 <--

56 : 3 = 18.6

56 : 2 = 2.5

On ne relève que les divisions entières. Il faudra essayer avec chaque longueur trouvée.

Pour la démonstration on prend directement la longueur de clé 8 qui donne 7 lignes.

On prend le texte crypté et on l'écrit en colonnes : les 7 premières lettres dans la 1ère colonne, les 7 suivantes dans la deuxième ...

NNDLI L?OLM T?SIJ ECEEL ENA?? SC?D? NUINE REEOM ?ROLT SSUS? ?E?SE A

N-O-J-N-D-R-O-?

N-L-E-A-?-E-L-?

D-M-C-?-N-E-T-E

L-T-E-?-U-O-S-?

I-?-E-S-I-M-S-S

L-S-L-C-N-?-U-E

?-I-E-?-E-R-S-A

Ensuite on effectue un anagramme des colonnes entières, c'est-à-dire qu'on déplace les colonnes pour retrouver l'ordre initial.

Si les espaces sont présents c'est une grande aide pour le décrypteur car deux ? ne peuvent pas se suivre. Cela permet aussi de délimiter les mots à rechercher.

En premier lieu il faut essayer de trouver la première colonne.

On regarde la première ligne : NOJNDRO?

Quel mot qui contient un espace peut-on faire ? Le mot peut ne pas être complet.

Les colonnes étant liées si on déplace un colonne, les lettres de toutes les lignes de la colonne se déplacent.

A la ligne 2 : N-L-E-A-?-E-L-?, on observe deux ?, donc deux espaces et les lettres L,E et E,L. On en déduit qu'il doit y avoir un mot (ou un bout de gros) avec LE séparé par des espaces. Le bout de mot doit être la fin du mot de la première colonne.

C'est en déplaçant les colonnes et en vérifiant que le résultat a un sens sur toutes les lignes que l'on casse la transposition simple à rectangle complet.

Ce système n'offre pas de sécurité.

La DOUBLE TRANSPOSITION offre plus de sécurité. On récupère le texte codé la première fois et on le réécrit en tableau comme s'il s'agissait du texte clair avec une nouvelle clé. On a donc deux clés différentes de longueur différente. Une pour la première transposition, une pour la deuxième. Le texte chiffré est le texte qui sort de la deuxième transposition.

On peut aussi augmenter la difficulté en ne remplissant pas la dernière ligne du tableau, on parle alors de transposition à rectangle incomplet ou de transposition à colonne non pleine.

Cela inclut des décalages dans le texte crypté et empêche l'attaque par la division entre la taille du texte crypté et les longueurs possibles de la clé.

Si on veut casser le système il faut essayer toutes les longueurs de clés.

Si on prend un tableau à rectangle incomplet avec deux clés identiques le décryptage est possible en essayant de deviner le texte clair non pas sur une ligne mais sur deux à trois lignes.

La double transposition avec deux clés diffuse le mot codé sur trois lignes (si on connaît déjà la bonne taille).

Par contre si la double transposition à rectangle incomplet est utilisée avec deux clés différentes et mieux deux clés différentes de longueurs différentes, chaque mot est diffusé dans tout le texte crypté (avec la bonne longueur de clé) et on ne peut pas déterminer à la main quelle est la bonne longueur de clé.

Il est tout de même possible de casser le système avec des ordinateurs ou des machines électro-mécaniques (comme durant la dernière guerre) qui effectuent des analyses statistiques non plus sur un seul texte crypté mais sur de nombreux tous chiffrés avec les deux mêmes clés différentes.

Je joins le programme DOUBLE.EXE pour PC qui permet de coder un texte selon la méthode de double transposition à rectangle incomplet à partir de deux clés que vous choisissez.

Un conseil ne choisissez pas deux clés identiques !

Remarque : à partir de deux clés d'au moins 50 caractères et si le nombre de textes codés avec ces mêmes deux clés ne dépasse pas 5, il n'est pas possible de casser le système sauf à disposer d'une forte puissance de calcul comme les systèmes CRAY.

LE CHIFFREMENT PAR TRANSPOSITION MODIFIEE

Voici une description du code NPC (Normal Pukall Cipher) et du code EPC (Enhanced Pukall Cipher) développés tous deux par Alexandre PUKALL en 1989. Ce sont tous deux des améliorations des systèmes de transposition permettant de réduire la longueur de la clé tout en gardant une très forte sécurité.

Un texte codé en EPC Mode 1 avec deux clés différentes pour la première phase qui sont réutilisées pour la deuxième phase, doté d'un prix de 3000F a été diffusé en 1996 sur Internet. Les deux clés ne dépassaient pas 15 caractères. Personne n'a réussi à le casser. Pas même Jim Gillogly, Président de l'ACA (American Cryptographic Association) qui s'est attaqué au texte codé avec comme renfort plusieurs ordinateurs. Le texte codé est joint plus bas. Le concours est toujours ouvert. Mon adresse est incluse dans le texte crypté.

Je considère le chiffre EPC sûr contre les attaques moyennes (grandes entreprises) avec un clé de 15 caractères en EPC mode 3. (le texte codé doté de 3000F de prix devrait donc pouvoir être cassé puisqu'il n'est codé qu'en EPC mode 1. Avis aux amateurs !)

Le code NPC est une transposition par tableau incomplet avec un relèvement dépendant de la clé et un sous-relèvement dépendant d'une deuxième clé.

Premièrement il faut créer la première clé :

On prend un mot ou une phrase (par exemple):

CODERUNTEXTECESTBIEN (Coder un texte c'est bien)

Ensuite on créé une clé numérique a partir de cette phrase.

Sous chaque lettre on note la place de cette dernière par rapport a l'alphabet.

Si on a C Z F, le C=1, le Z=3, le F=2, ce qui donne 1 3 2.

Ceci car C est la premiere lettre dans l'alphabet par rapport a Z et F. F est la deuxieme lettre dans l'alphabet par rapport a C et Z et Z est la troisieme.

Si une lettre se repete plusieurs fois dans la phrase, la lettre la plus a gauche prend la premiere place et ainsi de suite.

Si on a : C Z F Z F Z on aura C=1, Z=4, F=2, Z=5 ,F=3, Z=6.

Ce qui donnera 1 4 2 5 3 6 comme cle numerique.

Pour CODERUNTEXTECESTBIEN on aura :

C-O-D-E-R-U-N-T-E-X-T-E-C-E-S-T-B-I-E-N

2-13-4-5-14-19-11-16-6-20-17-7-3-8-15-18-1-10-9-12

On choisit ensuite une deuxieme cle (par exemple):

JAIMETOUJOURSMANGER (J'aime toujours manger)

On la transforme en cle numerique ce qui donne :

J-A-I-M-E-T-O-U-J-O-U-R-S-M-A-N-G-E-R

7-1-6-9-3-17-12-18-8-13-19-14-16-10-2-11-5-4-15

Il faut que la deuxieme cle soit toujours aussi longue que la premiere, si elle est plus courte, on repete la cle depuis le debut. Ici la deuxieme cle fait 19 caracteres, on repete donc un chiffre depuis le debut ce qui donne le 7 que l'on rajoute a la fin :

7-1-6-9-3-17-12-18-8-13-19-14-16-10-2-11-5-4-15-7

On utilise ensuite les deux cles comme une serie de cordonnees (X/Y)

X: 2-13-4-5-14-19-11-16-6-20-17-7-3-8-15-18-1-10-9-12

Y: 7-1-6-9-3-17-12-18-8-13-19-14-16-10-2-11-5-4-15-7

On cree ensuite un tableau de longueur de la premiere cle ou l'on ecrit le texte en clair :

\X 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20

Y

1 L A - D E R N I E R E - O F F E N S I V

2 E - D E V R A - S E - F A I R E - D A N

3 S - L E S - A R D E N N E S - B E L G E

4 S . L E S - T R O U P E S - S E R O N T

5 - P R E T E S - D E S - L A - V E I L L

6 E - . L E S - O P E R A T I O N S - C O

7 M M E N C E R O N T - A - C I N Q - Z E

8 R O - Z E R O . D U - C O M M A N D E M

9 E N T - S U P R E M E - A - B A S E - A

10 V A N C E E - T E R M I N E .

La cle X permet de selectionner la colonne du tableau et la cle Y permet de selectionner la ligne.

X: 2-13-4 .....

Y: 7-1-6 ......

On prend X/Y : 2 et 7 (on prend 7 modulo le nombre de lignes du tableau).

(Ici s'il n'y avait que quatre lignes (par exemple) on prendrait 7 % nombre de lignes donc 7 % 4 = 3.)

Revenons a notre exemple :

X/Y : 2 et 7.

Dans le tableau, la colonne 2 est la suivante :

A

-

-

.

P

-

M

O

N

A

La ligne 7 est la suivante :

M M E N C E R O N T - A - C I N Q - Z E

Voici les deux reunies :

A

-

-

.

P

-

-> M E N C E R O N T - A - C I N Q - Z E

O

N

A

La fleche -> designe l'intersection des deux.

Ici se trouve la lettre M.

La lettre M est la treizieme dans l'alphabet (M=13), voir le tableau ci-dessous:

A=1

B=2

C=3

D=4

E=5

F=6

G=7

H=8

I=9

J=10

K=11

L=12

M=13

N=14

O=15

P=16

Q=17

R=18

S=19

T=20

U=21

V=22

W=23

X=24

Y=25

Z=26

-=27

.=28

+=29

?=30

On effectue alors le calcul :

X + Y + lettre trouvee a l'intersection de la ligne et de la colonne, ici M, donc on a :

X + Y + val(M)

2 + 7 + 13 = RESULTAT = 22

Si RESULTAT est pair (even) alors on releve la colonne en descendant.

Si RESULTAT est impair (odd) alors on releve la colonne en montant

Ici RESULTAT est pair donc on releve la colonne en descendant, ce qui donne :

M O N A

On passe ensuite a la suite de la cle X/Y :

X/Y: 13 et 1.

A l'intersection de la colonne 13 et de la ligne 1, il y a la lettre O (valeur de O = 15).

X + Y + val(O) = 13 + 1 + 15 = 29

29 est impair on releve donc la colonne en montant :

Comme nous sommes sur la premiere ligne on ne releve qu'une lettre :

O

On passe a la suite :

X/Y : 4 et 6

4 + 6 + val (L) = 4 + 6 + 12 = 22

22 est pair, on releve donc la colonne en descendant :

L N Z - C

X/Y : 5 et 9

5 + 9 + val (S) = 5 + 9 + 19 = 33

33 est impair, on releve donc la colonne en montant :

S E C E T S S V E

On a depuis la debut releve les lettres :

M O N A O L N Z - C S E C E T S S V E

Soit en groupes de 5 :

/MONAO/LNZ-C/SECET/SSVE/.....

On continue ainsi de suite ...

A noter que dans les colonnes ou la derniere ligne est imcomplete, si le couple X/Y pointe sur cette ligne, on ne releve aucune lettre et on passe au couple X/Y suivant.

Une fois que tous les couples X/Y on ete releves, on recommence encore une fois depuis le debut et on releve le reste des lettres a l'inverse du premier relevement. Si on avait releve les lettres en montant pour cette colonne, on les releve a present en descendant (et inversement).

Avec X/Y: 2 et 7, on releve a present en montant :

- P . - - A

Avec X/Y: 13 et 1, on releve a present en descendant :

A E S L T - O A N

Avec X/Y: 4 et 6, on releve a present en montant :

E E E E D

Avec X/Y: 5 et 9, on releve a present en descendant :

E

Et ainsi de suite jusqu'a la fin des couples X/Y ...

POUR DECODER :

On fait l'inverse avec les lettres :

/MONAO/LNZ-C/SECET/SSVE/.....

On prend le premier couple X/Y : 2 et 7

et la premiere lettre des groupes : M

On fait le calcul

X + Y + val(M)

2 + 7 + 13 = RESULTAT = 22

22 est pair donc on sait que l'on va noter les lettres en descendant soit : dans la colonne au point (2;7) en descendant jusqu'en bas de la colonne, soit 4 lettres : M O N A.

On continue ainsi pour tous les couples puis on revient a nouveau au debut et on refait un passage avec les groupes et qui restent en remplissant l'inverse des colonnes. On reconstitue ainsi le tableau complet qui contient le texte clair.

A noter que pour decoder, il faut imperativement connaitre combien de cases ne sont pas remplies dans la derniere colonne. Pour cela on compte le nombre de lettres du texte crypte, ici 195 lettres. On sait qu'il y a 20 colonnes grace au nombre de lettres de la premiere cle, on divise alors 195/20= 9,75

On sait qu'il y a 9 colonnes completes de 20 caracteres chacune.

9*20=180

180-195=15 cases qui sont remplies sur la derniere ligne. Les 5 dernieres cases de la derniere ligne ne devront donc pas etre utilisees.

Ceci est le chiffre NPC mode 1 (Normal Pukall Cipher mode 1).

Le chiffre EPC mode 1 (Enhanced Pukall Cipher mode 1) est la meme chose mais en double transposition. C'est a dire que lorsque l'on a fini l'operation de codage complete, on prend le resultat et on le recode a nouveau avec les deux memes cles. Ce mode est plus long mais aussi plus sur.

Enfin, le chiffre EPC mode 3 (Enhanced Pukall Cipher mode 3) est la meme chose que le chiffre EPC mode 1 mais lors de l'operation de double codage on prend deux cles differentes par rapport aux deux premieres cles. On utilise donc dans ce mode 4 cles differentes.

Ce mode est encore plus sur que le mode precedent. Il semble egalement que le chiffre EPC permet de rendre la double transposition sure meme avec des cles relativement courtes (15 a 20 caracteres) alors qu'il fallait des cles beaucoup plus longues en double transposition normale.

Voici un texte code en NPC mode 1, sans separations (-) entre les mots :

DEBUT

ORISI / DERME / LOEEE / RNDNO / EEPRA / ITSUL / SEUOC / ELEDE / OSEGE / IRUEU / LTUUA / LEARP / RACLO / ROPRA / IETST / AUDEN / EUSMO / ROTTN / NNREF / NLEID / FEERE / EISNE / ROTO /

FIN

Voici un texte code en EPC mode 1, sans separations (-) entre les mots :

DEBUT

REHUA / AVRLL / CELYU / CAICC / ATNOP / TGBEX / RMETE / LLSDO / SEEQE / MACVD / EDFVE / ESENE / MLMPL / EICPU / TEIEM / NCPAP / ELEHT / OPNRU / CAUEA / DFSNS / REANC / CCDLE / RISEU / USESA / EIDTS / MLTOA / MIOGF / ULORD / STHUA / LEUSU / CANIL / AOMUP / IEALS / BNXLD / RIUEI / EECOE / EITDN / GCLDE / JENKE / GOEAP / ESLTD / IEZOR / SEELM / AO /

FIN

****

Voici le texte codé en EPC Mode 1 doté de 3000F de prix. Les / ne sont présents que pour séparer les groupes de 5 lettres et n'interviennent pas dans le texte codé. Les mots DEBUT et FIN n'interviennent pas non plus dans le texte codé.

A noter que les espacements sont présents ce qui devrait rendre possible le décodage. Pour l'instant personne n'a réussi à le décoder !

DEBUT

BOLEE / OAOIN / T-OI- / --ACL / --CIA / UTEC- / EMFDE / -TOOE /

UDS-- / RAREU / SED-- / NAEON / PFLUU / -TOCR / -EUAM / IPO-S /

ATADS / AVNVU / EIMSC / E--M- / SINEC / E-LS- / CLAUG / N--E- /

I-MED / USS-N / --UME / RDNET / LRMTE / -JLHE / SMSNE / -ESG- /

----S / -EHNN / O-U-- / RAEV- / RM-NM / V-IE- / IIE-E / -TEJI /

E-NE- / EE-NR / ZO-CD / OAULT / OOA-- / -SEAE / EET.U / -RBN- /

--A-U / CI--C / ODSTN / NAUUE / AROCH / R-OT- / MSECR / UEQE- /

SEO-O / TMSL- / QATAR / IS-RS / IETJI / UCEYR / EE-IU / T-OZU /

NGESS / LJXAV / OACSC / EUDTS / ISDRG / OSIEE / HOEZR / STUTD /

L-C?E / SENUN / MA-AE / LNLLE / MDDHE / PAU-E / -EDTE / UIOGT /

-PUI- / -VNMA / G-U-- / TA--R / SLVEL / --NAR / M-LAO / FAACB /

FL6-N / EDFLE / --NST / ETEE- / LVQLS / RLCIQ / I---- / LEYLN /

-SUEA / I--D- / AOIEI / RDEBQ / NEVEI / TSVAI / T-ONL / UUZ-E /

DS-IL / R-EV- / S---- / -EOME / --RTR / --AMO / I-EP- / ALANE /

SMR-A / --VSS / E--O- / R-TVU / ERDOS / NMUTF / T--E- / ESOTH /

IS-ME / ERVBS / O--SO / NNLT- / -PA-S / MYNES / EICSN / RLBOO /

ARUPO / PDTIE / ETQEU / EESCO / ODRPS / UMREI / EFNEA / T-COM /

E-UDT / --CBD / EEAAH / LRI-E / SCND- / HIEAI / FR-EF / OLEDN /

-O-PE / -LIOC / -NARE / DASDT / VECAF / B-SNV / E-ESV / SLLE- /

LA-EA / MNAEE / ECS-S / .IEUA / NEC-- / L-OCI / DUU-C / ENEOC /

-EEML / LTIO- / -ABD- / O--S- / NPQ-E / DITEA / -E-JL / NING- /

1OE-M / .D-AT / EOESF / TTNCM / DRU-E / V-IEE / AFUGN / NI-NE /

AEDEA / AUOEI / TAGNR / EAECU / P-HOP / AGEOT / AEELI / OQV-E /

EI-AZ / NAEPD / HS--E / ELTR. / USNRL / E-PME / QMA-N / MNYIA /

MPOES / DBP-L / UARRE / -TTNI / MTDMS / R-N.- / --TA- / -TID- /

EEEEL / TIEST / IAP-N / -ETEN / EAN-F / NO-NE / REN-E / EUS-- /

SUUTV / EPATI / RIAN. / FFERM / DSTES / EK-E- / C-ANA / N-SFA /

OBNME / EU-RO / -ESS- / -E-S- / IREEL / ONRE- / E-USS / SDJRE /

IO.NN / CNO-- / -RD9C / GENRJ / -L-HE / -SDI- / S--EL / --A.O /

DM--- / TC--- / NRR-S / -PNRR / RNEEO / NGCNI / F-M-A / ENEI- /

CAU-O / MO-AU / INDXA / T-CFO / F-LVC / OAVJI / ARDEH / S-IEU /

TOLB- / NEUL- / RTSSD / -L-AE / --TIN / AC-IE / DP.LO / SQAO- /

T--AU / -RLAD / -LENH / EE-E- / -RTMP / E-USO / -LELL / EIA.Z /

RRRUO / N-AOO / .LZGE / TJ-VT / COARP / DTQIE / EP--- / -AD-H /

EUIEE / -NAC- / EEEUE / -HILR / GNO-S / ---AN / UBIIE / EL-.- /

CCPST / SISSD / E-NGE / I-SEO / VE-N. / -D-SE / -FPSE / SS-EA /

-?9CU / HEE-- / NC-ER / T.HET / EOTEI / U-ILT / ES-EA / DO-L- /

TFO-E / --SEN / US--E / NOVRS / EEGK- / N-DRE / RI-TE / BNSQP /

S-ECV / EE-PO / IAEEL / EBUIC / LEEEP / R-I-- / -NT-I / EIEOE /

ESNOS / SU--S / -INOG / -ER-S / UI-TA / -EAEA / IICUM / TS-NS /

RUPC- / NI.EO / HOU-I / AE-EE / UCEPN / VREOI / PIATN / EYNVR /

RIRKC / S-NRE / SNT-- / IANUO / TMTAC / EVE-E / ESOSO / IPRUT /

-PLNN / -TOIL / OPTAC / R--FA / NDF-- / -I-C- / -?IEV / NTP- /

FIN

****

Si vous désirez vous exercer au "cassage" de systèmes de ce type, regardez le fichier CORRES.DOC joint, il contient toute une correspondance privée et encryptée par des méthodes manuelles.

LES MACHINES ELECTRO-MECANIQUES

ENIGMA :

Enigma était l'invention d'un Hollandais, Hugo Koch de Delft, qui avait pris un brevet pour une machine à écrire secrète, à La Haye en octobre 1919. Koch avait créé une société pour développer et exploiter son invention, mais incapable de mener à bien la réalisation de la machine, il avait cédé les brevets à un Allemand, Arthur Scherbius, ingénieur-inventeur habitant Berlin, qui avait construit effectivement une machine à partir des plans de Koch et l'avait appelée Enigma d'après les " Variations sur une énigme " de Sir Edward Elgar.

Ce prototype de Scherbius, forme assez primitive de la machine chiffrante à rotors définitive, avait été exposé au public pour la première fois en 1923 au Congrès du Syndicat international des Postes et en 1924 les Postes allemandes avaient utilisé une Enigma pour échanger des voeux avec le congrès.

Selon une brochure diffusée en anglais, la machine était conçue à l'origine pour protéger les secrets commerciaux et non les secrets militaires, et ses mérites étaient vantés comme suit :

" La curiosité naturelle de vos concurrents sera déjouée par une machine qui vous permettra de garder entièrement secrets tous vos documents, tout au moins les plus importants d'entre eux, sans occasionner de dépenses notables. Un secret bien protégé peut vous faire récupérer totalement le prix de la machine ... "

Malheureusement pour lui l'entreprise hasardeuse de Scherbius n'eut aucun succès et il vendit les brevets d'Enigma à une autre compagnie.

Entre-temps, Hitler était arrivé au pouvoir. Aussi le réarmement et la réorganisation de la Wehrmacht allaient-elles bon train. Les généraux battaient la campagne pour trouver des laboratoires et des ateliers susceptibles de fournir une nouvelle machine à coder capable de protéger leurs secrets.

C'est la Colonel Erich Fellgiebel, appelé à devenir l'officier en chef des transmissions de l'armée allemande et du Haut Commandement allemand, qui, le premier, prit fait et cause pour Enigma. Fait significatif, Fellgiegel allait également devenir l'un des conspirateurs les plus actifs de la Schwarze Kapelle.

Enigma disparut alors des circuits commerciaux et dès que Fellbiegel se mit à l'expérimenter, elle se révéla peu onéreuse, solide, portative, simple à manoeuvrer, et apte à fournir des codes en abondance. Mais par-dessus tout, après avoir rajouté à un tableau de clés électriques, on la proclama à l'abri des tentatives de décryptage les plus poussées. Ainsi était-il relativement peu important qu'elle fût saisie par un ennemi puisqu'elle se révélait inutilisable sans les clefs de codage. Elle répondait donc exactement en tous points aux besoins de la Wehrmacht.

Comme on le sait maintenant les anglais avec l'aide de machines électroniques dédiées réussirent à casser Enigma durant toute la guerre.

La machine à chiffrer Enigma automatise en fait un procédé de substitution polyalphabétique avec une longueur de clé très très longue : elle utilise des moyens mécaniques et électriques associés à un clavier mais ne comporte pas de dispositif d'impression.

Elle est basée en fait sur le principe du tambour chiffrant ou rotor. Un rotor est un disque de la taille approximative d'un palet de hockey, fait d'un matériau isolant et munit sur chaque face de 26 contacts électriques. Un ensemble de connexions arbitrairement choisies relie chaque contact de la face d'entrée à l'un des contacts de la face de sortie. Sachant que chacun de ces contacts correspond à une lettre, il est clair qu'un rotor n'est rien d'autre que la réalisation électrique d'un alphabet de substitution de type monoalphabétique à alphabet désordonné.

Mais si on le fait tourner entre deux disques fixes portant, eux aussi, 26 contacts, on obtiendra 26 alphabets de substitution différents. On en aura 676 (26*26) si, entre les deux disques fixes, on juxtapose deux rotors tournant à un rythme différent (cas d'Enigma grâce aux 'doigts d'entraînement'), et ce nombre est multiplié par 26 pour chaque adjonction d'un rotor supplémentaire :

trois rotors : 17576 alphabets

quatre : 456976

cinq : 11 881 376.

Le mérite particulier de ce dispositif réside donc dans l'énorme quantité d'alphabets de substitution qu'il peut produire. Comme la position relative des rotors varie constamment (les rotors tournent dans un mouvement semblables à celui des roues d'un compteur), chaque lettre d'un texte clair, même prodigieusement long, peut être chiffré avec un alphabet différent.

Et c'est là l'astuce d'Enigma : un seul alphabet est une substitution monoalphabétique facilement cassable. Mais s'il y en a des milliers et que chaque lettre est chiffrée avec un alphabet différent cela devient une énorme substitution polyalphabétique impossible à casser car la clé (fournie par les rotors) est aussi longue que le texte clair.

Enigma a cependant été cassée par les premiers ordinateurs au monde entre 1939 et 1945.

Ensemble mécanique : Un clavier, trois tambours (ou rotors) et un système d'entraînement des tambours constituent l'ensemble mécanique.

Le clavier à 26 touches (lettres majuscules uniquement, pas de barre d'espacement) est le même que celui d'une machine à écrire de type allemand (QWERT ...).

Chaque touche du clavier est directement reliée à un système de levier portant un axe sur lequel peuvent pivoter trois doigts d'entraînement dont les extrémités supérieures sont terminées par un bec.

Les doigts, dans certaines positions bien déterminées, entraînent les tambours (ou rotors) et les font avancer d'un pas.

Les tambours mobiles sont constitués chacun d'un noyau et d'une couronne crantée à 26 secteurs portant les 26 lettres de l'alphabet normal (A à Z). Chaque couronne alphabétique peut tourner et occuper 26 positions relatives par rapport au noyau.

Ensemble électrique : L'ensemble électrique comprend une alimentation, 26 circuits et 26 lampes correspondant aux 26 touches du clavier.

Le courant est fourni soit par des piles soit par le secteur, au moyen d'un transformateur.

Je joins le programme ENIGMA4.EXE, l'algorithme provient d'une machine ENIGMA de la Wehrmacht.

Il faut savoir que les machines ENIGMA ont été décodées par les Alliés durant la seconde guerre mondiale. Cependant, les rotors internes de la machine étaient câblés en usine et aucune modification ne pouvait y être apporté par la suite. La sécurité de la machine dépendait de la façon d'installer trois rotors parmi cinq au choix et de la façon de connecter des fils électriques sur un tableau de sécurité.

J'ai modifié l'algorithme en gardant non seulement les systèmes de l'époque mais en plus le 'câblage' logiciel des rotors change en fonction des clés de cryptage. Il change non pas

chaque fois que l'on change les clés mais à chaque nouvel octet crypté. Pour un fichier crypté on a donc (26!)^3 soit factorielle de 26 puissance 3 possibilités soit 6E79 possibilités soit un nombre commençant par 6 et suivi de 79 zéros. Durant la seconde guerre mondiale ce nombre était réduit à (13!)*6! soit 13! * 720 soit 4E12 soit 4 suivi de 12 zéros seulement. (13! pour les 13 câbles électrices utilisés. Le calcul n'est pas exact, la formule pour déterminer les différentes façons de connecter les câbles est plus longue mais cela donne une idée).

Les machines de Türing parvenaient donc à trouver le bon code après 4E12 essais soit 4000 milliards d'essais.

Cependant entre 4E12 essais et 6E79 il y a un gouffre que personne n'est prêt de franchir. (A noter qu'il y a environ 1E80 étoiles dans notre univers).

Ceci démontre donc qu'on ne peut attaquer le système depuis le message codé il faut donc attaquer la clé, c'est-à-dire essayer toutes les clés possibles. Le nombre de possibilités de clés est cependant beaucoup moins grand que le nombre de codages différents d'un même texte clair. Deux clés sont demandées, une clé numérique de 32 bits et une clé alphanumérique de 64 bits soit 96 bits. Le nombre de clés possibles est donc de 2^96 (2 puissance 96) soit 7E28 soit 70.000 millions de milliards de milliards de possibilités. C'est vrai que c'est moins que 6E79 mais c'est déjà pas mal.

LE CHIFFREMENT MODERNE PAR ORDINATEUR

Les ordinateurs ont totalement modifiés la donne en ce qui concerne la cryptographie.

En effet, grâce à lui on peut créer des algorithmes très puissants et très faciles à mettre en oeuvre puisque c'est l'ordinateur qui fait tous les calculs.

Voici l'algorithme de chiffrement en continu PC1 (Pukall Cipher 1), vous pouvez l'utiliser gratuitement à condition de mentionner le nom de l'algorithme et le nom de l'auteur dans le logiciel final.

L'algorithme est écrit en C mais peut être adapté à d'autres langages.

L'algorithme est très puissant et utilise une clé de 10 octets (chaque octet peut avoir n'importe quelle valeur de 0 à 255). Il peut, bien sûr, coder aussi bien des fichiers textes, que des images ou des programmes exécutables.

Il est utilisé commercialement (j'ai offert le code source gratuitement) dans plusieurs applications.

Il est également présent dans plusieurs logiciels Freeware. Je joins le logiciel PEDIT qui est un éditeur de texte pour MS-DOS incluant l'algorithme PC1. Il est en anglais. Pour activer le cryptage il faut taper sur CRTL-P puis entrer deux fois le mot de passe.

L'algorithme PC1 est incassable dans l'état actuel de la technique. Un texte crypté par PC1 est joint et se nomme SORTIE.TXT

Le symbole ^ correspond à l'instruction XOR (en pascal)

Le symbole % correspond à l'instruction MOD

Le symbole == correspond à l'instruction de test égal. if (a==b) est équivalent à si a=b ...

Le symbole a=5 correspond à l'affectation a:=5 (en pascal)

L'instruction : for (compte=0;compte<=9;compte++) correspond à POUR COMPTE=0 ALLER JUSQU'A COMPTE <=9 avec COMPTE=COMPTE+1 à chaque fois.

Le symbole >> correspond à l'instruction de décalages de bits vers la droite. e>>8 correspond à décaler la variable e de 8 bits vers la droite et à lui affecter le résultat.

Le symbole & correspond à un ET logique. (AND)

Une variable de type :

int varie de -32768 à 32767

unsigned int varie de 0 à 65535

unsigned long varie de 0 à 4294967295

char varie de -128 à 127

unsigned char varie de 0 à 255

short varie de -32768 à 32767

unsigned short varie de 0 à 65535

```
/* Fichier PC1.c */

/* ecrit en Borland Turbo C 2.0 sur PC */

/* Algorithme de CODAGE PC1 ( Pukall Cipher 1 ) */

/* (c) Alexandre PUKALL 1991 */

/* Utilisation et modifications libres si le nom de l'auteur est */

/* inclu dans le programme final et la documentation du logiciel */

/* dans un endroit accessible librement par l'utilisateur comme */

/* les fenetres A propos des logiciels sous Windows sur PC */
```

```
/* Cet algorithme a ete ecrit en Assembleur 6809 Motorola */

/* le code C ci-dessous est la traduction rapide de cet algorithme */

/* le fonctionnement est identique */

#include <stdio.h>

#include <string.h>

unsigned int ax,bx,cx,dx,si,tmp,x1a2,x1a0[5],res,i,inter,cfc,cfd,compte;

unsigned char cle[11]; /* les variables sont definies de facon globale */

short c;

FILE *in,*out;

fin()

{

/* on quitte en effacant toutes les variables utilisees par l'algorithme */

for (compte=0;compte<=9;compte++)

{

cle[compte]=0;

}

ax=0;

bx=0;

cx=0;

dx=0;

si=0;

tmp=0;

x1a2=0;

x1a0[0]=0;

x1a0[1]=0;

x1a0[2]=0;

x1a0[3]=0;
```

```
x1a0[4]=0;

res=0;

i=0;

inter=0;

cfc=0;

cfd=0;

compte=0;

c=0;

exit(0);

}

assemble()

{

x1a0[0]= ( cle[0]*256 )+ cle[1];

code();

inter=res;

x1a0[1]= x1a0[0] ^ ( (cle[2]*256) + cle[3] );

code();

inter=inter^res;

x1a0[2]= x1a0[1] ^ ( (cle[4]*256) + cle[5] );

code();

inter=inter^res;

x1a0[3]= x1a0[2] ^ ( (cle[6]*256) + cle[7] );

code();

inter=inter^res;

x1a0[4]= x1a0[3] ^ ( (cle[8]*256) + cle[9] );;

code();

inter=inter^res;
```

```
i=0;
}
code()
{
dx=x1a2+i;
ax=x1a0[i];
cx=0x015a;
bx=0x4e35;
tmp=ax;
ax=si;
si=tmp;
tmp=ax;
ax=dx;
dx=tmp;
if (ax!=0)
{
ax=ax*bx;
}
tmp=ax;
ax=cx;
cx=tmp;
if (ax!=0)
{
ax=ax*si;
cx=ax+cx;
}
tmp=ax;
```

```
ax=si;

si=tmp;

ax=ax*bx;

dx=cx+dx;

ax=ax+1;

x1a2=dx;

x1a0[i]=ax;

res=ax^dx;

i=i+1;

}

main()

{

int encode;

si=0;

x1a2=0;

i=0;

encode=1; /* mettre à 1 si on veut coder, à 0 si on veut décoder */

/* C'est le cle ci-dessous ('Remsaalps!') que vous pouvez changer */

strcpy(cle,"Remsaalps!"); /* copie les 10 caracteres de la cle dans cle */

/* ouverture du fichier ESSAI.TXT qui sera code-decode */

/* il doit exister un fichier ESSAI.TXT dans le repertoire courant ! */

/* a vous de le creer ! */

if ((in=fopen("essai.txt","rb")) == NULL) {printf("\nErreur lecture fichier ESSAI.TXT !\n");fin();}

if ((out=fopen("sortie.txt","wb")) == NULL) {printf("\nErreur d'ecriture fichier SORTIE.TXT !\n");fin();}

/* le fichier code se trouve dans SORTIE.TXT */

while ( (c=fgetc(in)) != EOF) /* la variable c recoit l'octet lu dans le fichier */
```

```
{
assemble(); /* execute la routine de codage */
cfc=inter>>8;
cfd=inter&255; /* cfc^cfd = octet aleatoire */
if (encode==1)
{
/* ici le melange de c ( octet clair ) avec cle[compte] se situe */
/* avant le codage de c */
for (compte=0;compte<=9;compte++)
{
/* on melange l'octet clair lu dans le fichier */
/* a la cle utilisee pour le codage */
cle[compte]=cle[compte]^c;
}
c = c ^ (cfc^cfd);
}
if (encode==0)
{
/* ici le melange de c ( octet clair ) se situe apres le */
/* melange avec cle[compte] car il faut decoder d'abord */
/* l'octet chiffre */
c = c ^ (cfc^cfd);
for (compte=0;compte<=9;compte++)
{
/* on melange l'octet clair lu dans le fichier */
/* a la cle utilisee pour le codage */
cle[compte]=cle[compte]^c;
```

```
}

}

fputc(c,out); /* ecriture de l'octet code-decode dans le fichier SORTIE.TXT */

}

fclose (in);

fclose (out);

fin();

}
```

Alexandre PUKALL

N.B :

/ REALH / SIHTR / --R-I / ULEEU / -REB- / RSHWN / DLEUF / -NEEL / -RT-E / LI /