La cryptographie

ihre Wirksamkeit sollte einsetzen, sobald die V 2 aus der senkrechten Lage durch eine Programmsteuerung in die Flugbahn eingefädelt war. Dann übernahm das «drahtlose Kanonenrohr» die Führung bis zum Kommando «Brennschluss», das auf Grund der Entfernungsmessung automatisch gegeben wurde.

Schwieriger war die Aufgabe, Flakraketen, wie «Wasserfall», «Enzian», «Schmetterling» und «Rheintochter», zu steuern. Nur wenige vollständige Flakraketenbatterien mit Fernsteuereinrichtungen (zu vier Abschußstellen) sind geliefert worden. Ein normales Funkmessgerät diente der Erfassung des Zieles in einem Sichtgerät mit Fadenkreuzanordnung und wurde ständig so auf das Ziel gerichtet, dass dieses in der Mitte des Fadenkreuzes erschien. Ein Funklenkgerät, gleichfalls dem «Würzburg» ähnlich, gestattete die Steuerung der Flakrakete nach Höhe und Seite mit Hilfe einer Knüppelsteuerung, wobei ein Empfängersender die Lage der Rakete auf dem Fadenkreuz-Sichtgerät vermerkte. Mit Hilfe der Knüppelsteuerung konnte der Leuchtpunkt der Flakrakete mit dem Leuchtpunkt des fremden Zieles in Deckung gehalten werden. Für die letzten Kilometer bis zum Ziel war in der Rakete ein zielsuchendes Funkmessgerät («Schnüffel») vorgesehen, das bis zur Wirkung des Abstandzünders die Führung übernehmen sollte.

Ähnliche Aufgaben bestanden für die Führung von Jägerraketen bei Tag und Nacht gegen Bomber. Zunächst erfolgte die Steuerung der Jagdrakete durch einen Draht, der sich aus der Rakete heraus abspulte. Wegen der Gefährdung des eigenen Gebietes, insbesondere der Hochspannungsleitungen, wurde auf eine Funkentwicklung umgeschaltet. Die Grundlage dazu gab die für gelenkte Bomben entwickelte Knüppelsteuerung. Der Bordsender (auf 7-m-Welle) hatte die Bezeichnung «Kehl», der Empfänger hiess «Strassburg». Dieses Verfahren brachte grosse Treffgenauigkeit und wurde Ende des Krieges auf 25 cm umgestellt.

Die Arbeiten auf dem Radargebiet sind zurzeit noch in Deutschland verboten. Die Radaraugen der modernen Navigation auf See und in der Luft sind in den Bereich des friedlichen Verkehrs hinübergewechselt. Dicht nebeneinander liegt auf den Gebieten der modernen Naturwissenschaften die Verwendung für Krieg und Frieden.

La cryptographie

De tous temps, les princes, les conspirateurs, les banquiers, les prisonniers et les soldats ont eu recours aux écritures secrètes pour empêcher leurs concurrents ou leurs adversaires de connaître leurs projets. Le secret des messages consiste parfois à les dissimuler dans une cachette, à les écrire à l'encre sympathique, à semer des signes convenus dans un texte d'apparence anodine, etc....

Ces procédés offrent une sécurité limitée et leur rendement est faible. C'est pourquoi on renonce parfois à dissimuler le caractère secret du message, et on le transforme en une suite, incohérente en apparence, de chiffres ou de lettres suivant une convention qui n'est théoriquement connue que du destinataire. Le cryptogramme ou message chiffré peut être expédié par n'importe quel mode de transmission : par la poste, ou, après découpage en tranche de 5 lettres, par télégraphe ou radio. A l'arrivée, le message subit entre les mains d'un déchiffreur le traitement inverse de celui qui l'a rendu incompréhensible. Le déchiffrement est une opération mécanique, qui demande seulement de la méthode. Mais un message chiffré est certainement très important et l'ennemi s'efforcera d'en pénétrer le sens. L'opération est infiniment plus délicate pour lui, puisqu'il lui faut deviner simultanément le texte clair et la convention qui a servi à le transformer, c'est le travail de spécialistes avertis appelés décrypteurs.

L'histoire du déchiffrement est une longue compétition toujours indécise entre chiffreurs et décrypteurs. Elle est fertile en anecdotes amusantes ou tragiques. Chiffreurs et décrypteurs ont, tour à tour, remporté des succès spectaculaires et l'aspect presque miraculeux de ces succès a plusieurs fois inspiré les écrivains et en particulier les auteurs de romans policiers. Les inventeurs aussi ont attaqué souvent, avec plus de confiance que de savoir, le problème du chiffrement et cru découvrir des méthodes « nouvelles » et « infaillibles », que le cryptologue rangeait immédiatement parmi les plus élémentaires des procédés connus.

Les procédés de chiffrement sont en nombre théoriquement infini, mais on peut les classer en systèmes auxquels le décrypteur sait appliquer les traitements convenables. Retenons donc qu'on n'a pas encore trouvé — même en utilisant les machines à chiffrer les plus perfectionnées — ni de système de chiffrement qui donne une sécurité absolue, ni de méthode de décryptement infaillible.

Systèmes élémentaires de chiffrement

Le chiffrement utilise deux opérations fondamentales qui peuvent être employées isolément où combinées :

— La **transposition** consiste à changer l'ordre des éléments, par exemple les lettres d'un texte clair de façon à le rendre incohérent en apparence;

— La **substitution** consiste à remplacer les éléments du texte — lettres, mots ou syllabes — par d'autres éléments qui peuvent être des lettres, des mots, des chiffres ou des signes quelconques, puisés dans des répertoires (codes ou dictionnaires) ou formés en appliquant certaines règles.

L'un des plus anciens procédés de chiffrement comme la scytale des Grecs était une machine à chiffrer consistant en une règle de bois sur laquelle on enroulait un ruban. On écrivait alors le message suivant les faces de la règle, et le ruban déroulé portait alors un texte dont les lettres avaient été transposées. Pour le lire, il suffisait au destinataire d'enrouler le ruban sur une règle identique à celle de l'envoyeur, et à lire suivant les faces. Un décrypteur moderne se contenterait de lire le texte en sautant à chaque fois le même nombre de lettres, ou d'écrire le texte par groupe de deux, trois, quatre... lettres pour former des tableaux rectangulaires où le texte apparaîtrait finalement en clair suivant les colonnes du tableau.

Le procédé de substitution le plus simple est dû à Jules César, il consistait à remplacer chaque lettre du texte par une lettre décalée d'un nombre constant de rangs dans l'alphabet : par exemple A par I, B par J, C par K, etc... Pour faciliter le chiffrement et le déchiffrement, on peut employer un dispositif un peu analogue à une règle à calcul, dans lequel deux réglettes coulissent l'une en face de l'autre. Chacune d'elles porte un alphabet prolongé de part et d'autre pour qu'on ait un recouvrement partiel. Si on change le décalage, il suffit de faire glisser une réglette le long de

Schang erzählt uns:

(10. Fortsetzung)

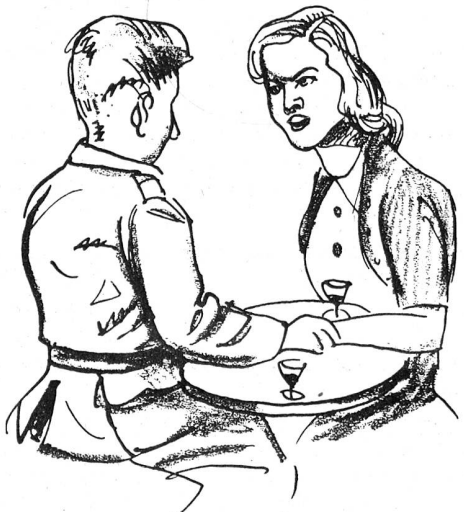
Q-Code-Lernen leicht gemacht

« Motto: Lerne es im Spiel . . . »

Freund Ted ist in letzter Zeit nicht mehr auf dem Band QRV — er soll sehr QRL military service, Rekrutenschule sein — und man hörte seine vertraute, jugendhafte Stimme schon lange nicht mehr im Äther.

Dafür entdeckten wir ihn kürzlich in einem QSO visu in der nahen Stadt, nahe unserer Stammbeiz, an einem Samstagabend. Schmuck sieht er aus in seiner feldgrauen Uniform; Pickfeiner Nachkriegsschnitt, mit den grauen Spiegeln links und rechts der Krawatte, Kittel in die Hüfte geschnitten, Säbel kurz und Hosen weit, Marke «Swing». Nur der Haarschnitt sieht nicht nach «Entenfudi» aus, oder wenn schon, dann eher nach einem gerupften . . . Mit ein klein wenig Neid denken wir an unsere steifen Ofenrohre, will sagen Hosenrohre daheim im Kleiderkasten, an das alte Sägemesser im lederverkleideten Futteral, das beim Laufschritt immer so blödsinnig schlänkert, und mit ein wenig Wehmut erinnern wir uns an unsere alten schwarzen Patten der Genietruppen mit dem goldenen Funkerblitz.

Aber zurück zum schmucken Ted, der nicht nur uns, sondern auch einer gutgewachsenen Blonden nicht übel zu gefallen schien. Ein QSO scheint bereits zu laufen, und am QRI, am taubenhaft girrenden Ton ihrer Stimme gemessen, scheint das QRK mindestens 5 zu sein.



Freund Ted kehrt uns den Rücken und ist so QRL mit seiner YL (young lady), dass er uns kaum bemerken wird. Gutes Band hier im Lokal, sehr QRO, gut ihrer sechs Mann, die nun wieder ihre Instrumente ergreifen und zu einem weiteren Modulationsversuch anheben. Ziemlich aufpeitschendes Spiel und gar nicht QSD, das muss man ihnen lassen. Ein Zittern durchläuft unseren Ted, und sein linker Fuss wippt bereits im Takt mit, also echt QLF (Taste jetzt mit dem linken Fuss!) — Er scheint ganz in sein Studium versunken zu sein. Jawohl Studium, und zwar Hochfrequenz-Technik. Sein Spezialgebiet, muss man wissen, ist die Erforschung der skin-Effekte. Auch hier kann er seinen wissenschaftlichen Eifer kaum lassen.

Der Kellner fragt uns nach unseren Wünschen, aber im QRM des Lokals geht unsere Stimme unter. Der Geräuschpegel ist in diesem QTH auch wirklich ausserordentlich hoch. Was sagt er, hier sei keine Schwachstrombeiz? Also mal her mit der Getränkekarte — — viel zu teuer für uns arme HAM-Brüder. Bestellen wir halt eine Flasche Roten, der ist noch am ehesten QRP. Aber, stellt euch vor, für den Betrag hätten wir eine viel edlere Flasche kaufen können, nämlich eine 807, deren Verkaufspreis unter Brüdern gerade etwa dem entspricht. Inzwischen ist Freund Ted verschwunden: er scheint QSY gemacht zu haben — wahrscheinlich etwas frische Luft schnappen, oder so. Auch das Orchester hat nach einem furiosen QRQ zur Abwechslung etwas QRT gemacht, und man kann sich wieder mit QSA 3 verständigen. Plötzlich taucht unser junger Kamerad mit holder Begleitung wieder auf und hat uns auch prompt erblickt. Was sagt er zu seiner Maid? «Bitte QRX, ich komme gleich wieder . . .» und schon setzt er sich an unseren Tisch. Dem Schmollmündchen an ist sie mit Ted nicht schlecht in Resonanz. Er aber schiesst gleich los, nachdem er uns mit unseren Rufzeichen begrüsst hat, wie das so allgemein üblich ist.

Es sei ein hochinteressanter Dienst, meint er, wenn auch sein Korporal manchmal sonderbare Auffassungen vertrete, wofür folgende Stilblüte zeugen solle; «. . . der Mast der G-anderthalb-K ist selbsterregt, und weil die ganze Hochspannung daranliegt, ist es lebensgefährlich, ihn anzurühren . . .» oder «. . . Die Ausbreitung der Wellen hängt vom Wetter ab: sie werden vom Nebel absorbiert, weshalb die Reichweite im Herbst geringer wird . . .»

Uns bleibt das Relais hängen ob der Tragweite dieser neuesten Erkenntnisse, die da an der Akademie im Unterland entdeckt werden. Wann er wieder einmal aufs Band komme, wollen wir von ihm wissen. Er aber meint, er und seine «Kollegen» hätten beschlossen, ihre Sender zu verkaufen samt der ganzen junk box (Radio-Grümpelkiste = schlechte Umschreibung für den liebevoll umhegten Schatz jedes echten Bastlers). Aus dem ersparten Sold werde dann eine UFB kommerzielle QRO Station gekauft, die auch etwas Saft abgeben könne, denn nur mit Saft lasse sich heutzutage etwas anfangen . . .

Dann gibt uns Ted noch die besten 73 auf und bittet uns, diese auch dem ganzen «gang» von der Ortsgruppe zu QSP-portugalen. Und mit einem freundschaftlichen «cheerio» wandte er sich wieder ab und war wieder für seine gelangweilt herumblickenden YL, QRV.

Bei aller Verwandtschaft mit Ted trennt uns doch ein grosser Abgrund. Wenn man eingefleischter Bastler und Selbstbauer ist, so gefallen einem solche Worte natürlich nicht besonders. Aber wir wollen ihm diese Einstellung lassen, wollen aber über das Problem «QRO oder QRP-Leistung»: Selbstbau oder Kauf später nochmals diskutieren.

Die QTR ist doch heute schon weit fortgeschritten, und als der Ober einkassieren kam, ist unser QSB im Portemonnaie derart ausgeprägt geworden, dass wir es vorziehen, für heute QRU zu sagen.

QTC next month, old boys,

Schang HB9CQ

---

l'autre pour obtenir la correspondance entre les lettres du clair et celles du cryptogramme. La réglette portant l'alphabet de substitution pourrait aussi porter un alphabet inversé, voire même incohérent.

Comment les décrypter?

Si nous nous reportons à une époque, antérieure à la Renaissance où les méthodes de chiffrement étaient encore assez rudimentaires, nous pourrons supposer qu'un décrypteur se trouve en présence d'un texte et se demande s'il a été transposé suivant le procédé simple que nous avons indiqué, ou s'il a été substitué par la méthode de Jules César. Malgré leur apparente incohérence, les cryptogrammes obtenus par ces deux méthodes présentent certaines particularités qui permettent au décrypteur de trancher la question : dans les procédés simples de substitution alphabétique, les lettres restent en place et se transforment toujours dans les mêmes lettres. Or, si nous supposons le texte écrit en français, toutes les lettres n'apparaîtront pas avec la même fréquence : le E est la lettre qui apparaît le plus souvent (14 % en moyenne), puis viennent (par ordre de fréquences décroissantes) les lettres S, A, R, T, I, N, U, L, O, C (l'ordre des quatre dernières étant contesté par les cryptologues). Si donc, dans un texte substitué par la méthode de César, une lettre apparaît avec une fréquence voisine de 14 %, nous aurons de bonnes raisons de croire qu'il s'agit d'un E. De même, les bigrammes (associations de 2 lettres) les plus fréquents sont ES (3 %), LE (2,4 %) et EN (2,4 %). Nous chercherons donc les bigrammes les plus fréquents, qui ont des chances d'être ces trois bigrammes et qui nous confirmeront que nous avons bien trouvé la lettre substituée à E. De même les lettres redou-

blées apparaissent dans l'ordre des fréquences décroissantes SS, LL, TT, MM..., le Q est presque toujours suivi d'un U. Toutes ces remarques permettront de faire rapidement une hypothèse sur la nature de l'alphabet de substitution et de deviner un certain nombre de lettres du clair. En se guidant sur ces lettres on complétera certains mots et on retrouvera peu à peu l'alphabet de substitution.

Si le texte a été transposé, les bigrammes se trouvent dissociés, mais les lettres demeurent inchangées et par conséquent le E sera le plus fréquent, suivi de S, A, R, etc. Nous saurons que nous avons affaire à une transposition et nous chercherons par tâtonnements à en déterminer la loi.

Si le chiffreur a transformé son texte en deux étapes: par une transposition suivie d'une substitution, on a affaire à un surchiffrement, le décryptement devient plus compliqué. Mais le décrypteur n'abandonnera pas et remarquera que la loi de fréquence des lettres reste inchangée par cette double transformation, et par conséquent aura déjà un fil conducteur. Puisque nous rencontrons un premier exemple de surchiffrement, disons tout de suite qu'il n'est efficace qu'à condition que les procédés de transformation employés soient bien distincts: si nous appliquons deux fois de suite à un texte une substitution du type Jules César, le résultat sera un texte écrit dans un alphabet décalé de la somme des décalages effectués, et par conséquent ne sera pas plus difficile à décrypter.

Le système de Vigenère

Quand les systèmes que nous venons d'indiquer furent éventés, il fallut trouver autre chose. On s'efforça de brouiller à la fois les bigrammes ou trigrammes caractéristiques du texte, ainsi que la statistique de fréquence des lettres. Ce progrès fut obtenu au moyen de systèmes plus ou moins ingénieux de décalage variable des alphabets de substitution.

C'est ainsi qu'au XVII^{e} siècle, le Belge Gronsfeld imagina de décaler chaque lettre du clair non plus d'un nombre re rangs constant comme dans le système de Jules César, mais variable suivant les indications d'une clef numérique.

Prenons par exemple la clef 21456. Le texte clair sera divisé en groupes de 5 lettres. Dans chaque groupe la première lettre sera décalée de 2 rangs, la deuxième de 1 rang, la troisième de 4, la quatrième de 5 et la cinquième de 6.

On voit sur cet exemple que les lettres répétées sur le texte clair cessent de l'être sur le cryptogramme. De même, on ne retrouve plus de lettre de fréquence caractéristique.

Bien qu'il lui fût postérieur d'une cinquantaine d'années, le système de Gronsfeld ne diffère pas dans son principe du système de Blaise de Vigenère, et il est d'une application moins aisée.

Vigenère imagina un tableau de lettres à 26 lignes et colonnes dans lequel il écrivait successivement les uns audessous des autres 26 alphabets qu'il décalait à chaque fois d'un rang vers la gauche par une permutation circulaire. Pour chiffrer un texte, il adoptait une clef formée d'un mot plus ou moins long ou de plusieurs mots. Le message étant écrit sous la clef de façon à établir une correspondance lettre à lettre, la lettre correspondante du cryptogramme était choisie à l'intersection de la colonne commençant par la lettre de la clef avec la ligne commençant par la lettre du clair. Ainsi E (clair) chiffré avec S (clef) donne W (en cryptogramme). On vérifiera aisément que l'exemple que nous avons donné du système Gronsfeld revient à chiffrer en Vigenère avec la clef littérale CBEFG, qui a l'inconvénient, étant incohérente, d'être difficile à retenir.

Le système Vigenère, inventé à la fin du XVI^{e} siècle, devait résister jusqu'au milieu du XIX^{e} aux efforts des décrypteurs. Quand il est bien employé avec une clef assez longue et des messages courts, on peut le considérer comme très sûr. On est toutefois parvenu à mettre au point une méthode de décryptement dont nous indiquerons le principe: Soit, par exemple, à chiffrer en Vigenère le texte du célèbre ordre du jour du général Joffre à la bataille de la Marne: «Au moment où s'engage une bataille . . .», etc., en utilisant comme clef le mot de huit lettres «VICTOIRE». Nous écrirons le texte en le découpant en tranches de huit lettres suivant un tableau rectangulaire. Les lettres situées dans une même colonne sont chiffrées avec la même lettre de la clef. Il en résulte que si certaines associations de lettres, bigrammes ou trigrammes se trouvent placées exactement l'une au-dessous de l'autre dans ce tableau, elles feront apparaître les mêmes associations de lettres transformées. Si on observe de telles répétitions dans un cryptogramme, il y a peu de chances qu'elles soient dues au hasard, et elles peuvent fournir un renseignement précieux: la longueur de la clef. En effet, si les associations de lettres considérées sont l'une sous l'autre dans le tableau, leur distance est un multiple de la longueur de la clef. Le décrypteur notera donc toutes ces répétitions, et en déduira la longueur de la clef.

Il pourra alors écrire le message chiffré sur 8 colonnes et saura que chacune d'elles a été chiffrée avec une même lettre-clef: ici la loi des fréquences des lettres reparaît et il sera vraisemblable que la lettre la plus fréquente sera la transformée d'un E. On essaiera par ces considérations de fréquence de deviner la lettre-clef, et on ne tardera pas à décrypter tout le message.

Il pourra arriver que la clef soit longue et le message difficile à décrypter. Mais si on possède plusieurs messages dont on a de bonnes raisons de croire qu'ils ont été chiffrés avec la même clef, on tirera d'utiles conclusions du fait que les lettres de même rang ont été chiffrées avec la même clef.

Dans la pratique, en effet, un message ne doit pas être étudié seul, mais confronté avec toutes les sources de renseignements qu'on possède. En particulier, il arrivera que l'on puisse presque affirmer que le message renfermera tel ou tel mot, par exemple: « bataille ». Dans ce cas on promènera ce mot tout le long du cryptogramme, et on verra quelle clef permettrait la transformation du mot « bataille » en une tranche de 8 lettres du cryptogramme, cette méthode du mot probable est d'un emploi général en cryptologie et rend de grands services.

L'autoclave

Pour compliquer la tâche du décrypteur, on a essayé de rendre la clef indéfinie. Une solution simple en apparence consisterait à se servir de deux exemplaires d'un même livre et à convenir du point de départ de la clef. Mais cette méthode est inapplicable en campagne. On a donc pensé utiliser, soit le texte clair, soit le cryptogramme pour prolonger la clef; c'est le procédé de l'autoclave.

La sécurité donnée par ce procédé est le plus souvent illusoire: si c'est le cryptogramme qui a servi à effectuer le chiffrement, on promènera cette clef le long du message et après quelques tâtonnements on trouvera d'un seul coup le texte clair.

Si le message a été chiffré avec le texte clair, on se rappellera que les lettres les plus fréquentes sont E et S, et que leur rencontre donne toujours W dans le cryptogramme. On relèvera les intervalles entre deux mêmes lettres du cryptogramme et l'intervalle le plus fréquent sera la longueur de la clef initiale, qu'on retrouvera après quelques tâtonnements.

(à suivre)