HAMFU
HISTORY

KRIEG IM AETHER

Vorlesungen an der Eidgenössischen Technischen Hochschule in Zürich
im Wintersemester 1976/1977
Leitung: Abteilung für Übermittlungstruppen, Divisionär A. Guisolan

Chiffriertechnik Heute

Referent: D. Stürzinger, Dipl. Ing.

Diese Vorlesung wurde durch die Stiftung HAMFU digitalisiert und als
PDF Dokument für www.hamfu.ch aufbereitet.

CHIFFRIERTECHNIK HEUTE

O. Stürzinger, dipl. Ing. ETHZ

1. HISTORISCHE SCHWERPUNKTE

Schrift ruft Geheimschrift. Seit der Zeit, da mehr als 2 Menschen schriftlich miteinander korrespondieren konnten, ergab sich der Bedarf, Meldungen vor Unberufenen zu schützen. Es existieren Keilschrifttafeln aus dem 3. Jahrh. v. Chr., die nachweislich gewisse Informationen in Chiffre enthalten. Es waren also einmal nicht die "alten Griechen", die die Chiffriertechnik erfunden haben, ja man fand Hinweise aus dem obern Niltal, die auf Geheimschriften schon im 9. Jahrh. v. Chr. schliessen lassen.

Wenn wir historisch weiter gehen, so kommen wir jetzt logischerweise doch zu den Griechen. Die haben die Problematik schon "wissenschaftlich" angepackt. Sie hatten einen Stab genommen (in Fig.1* als Polyeder dargestellt) - er kann auch rund sein - einen Streifen Papier schraubenförmig daraufgewickelt und den Text in parallelen Linien zur Längsachse aufgetragen. Hier haben sie den Spruch "HEUTE KEINE FEINDBERUEHRUNG usw." Wenn man den Streifen abwickelt, bekommt man eine sinnlose Folge von Buchstaben, womit auf den ersten Blick nicht viel anzufangen ist. Nur der Besitzer eines gleichartigen Stabes, auf den er den Streifen aufwickelt, kann den Text sofort rekonstruieren. Für den statistisch orientierten Leser allerdings kommt hier sofort eine Spracheneigenart zum Vorschein; die Häufigkeit der Buchstaben. Die deutsche Sprache hat den Laut "E" als häufigsten; zufälligerweise liegen hier gleich vier beieinander. Geschichtlich ein Stück weiter kommen wir natürlich zu den Römern, und ihr erster Kaiser, Julius Cäsar selber, hat ein Verfahren vorgeschlagen - es heisst heute noch im Fachjargon der "Cäsar" - nämlich eine Verschiebung der Textbuchstaben im lateinischen Alphabet um 3 Schritte (Fig.2).

* Eine genaue Identifizierung der Figuren befindet sich am Ende dieses Textes.

"Krieg im Aether", Folge XVI

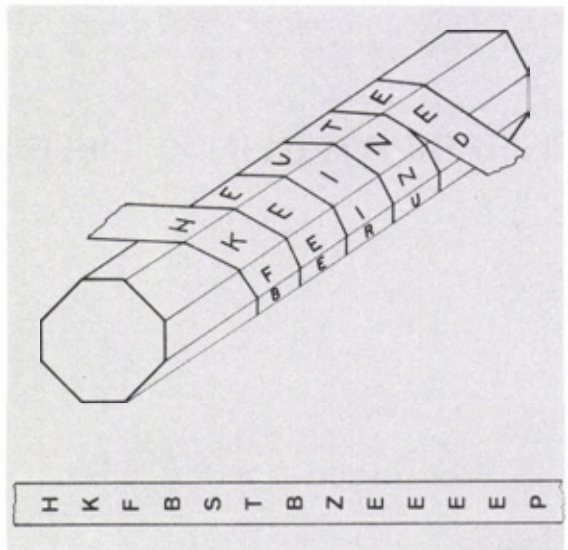


Fig. 1

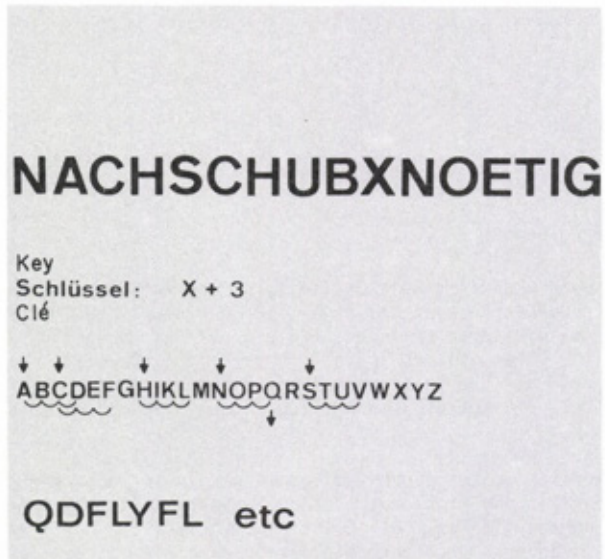


Fig. 2

Solche Verfahren hat der Leser wahrscheinlich schon in der Schule als Kind "erfunden", es ist heute also nicht mehr als hohe Technik zu betrachten.

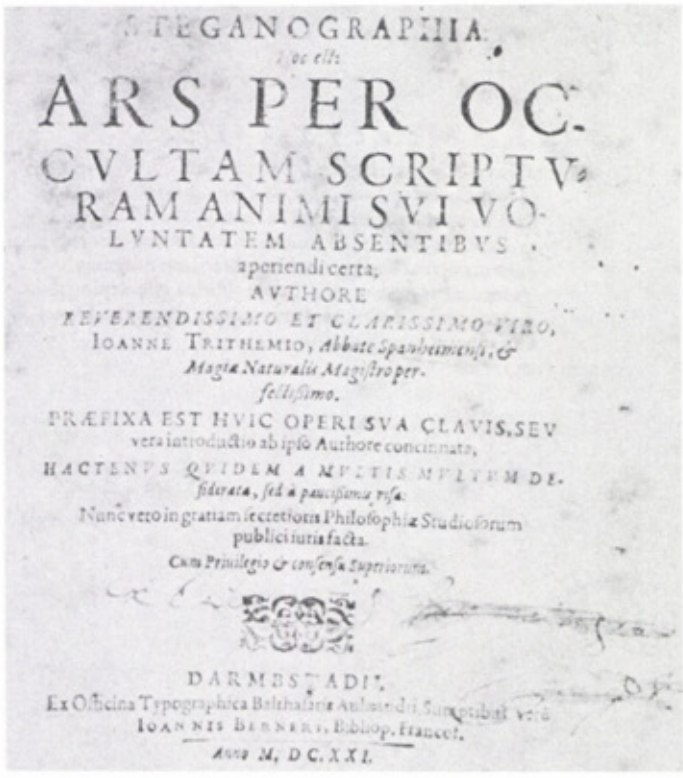
Weiter in der Geschichte kommen wir zu den Skandinaviern, genauer zu den Wikingern und offenbar liegt "Grund und Boden" im Norden ein bisschen anders auf diesem Gebiet, die Firma CRYPTO AG stammt ja, gegründet durch B.C.W.Hagelin, ursprünglich aus Schweden. Da wäre der sogenannte Röckstone (Fig.3 auf der nächstfolgenden Seite) zu nennen, das ist ein Runenstein aus dem 9. Jahrhundert.

2-3

Fig. 3

Runensteine sind ja Grabmalsteine, auf welchen meistens die Geschichte des beigesetzten Helden festgehalten wurde. Der spezielle Stein hier trägt u.a. die Geschichte des Helden "Vämod", der da begraben ist, aber das Ganze ist chiffriert und durch den überlebenden Vater "Varin" festgehalten worden. Dazu kommen nun aber noch eine ganze Menge zusätzlicher Geschehnisse, offenbar wollte man möglichst viel auf einmal in dieser "Geschichtsbuchseite" geheim festhalten. Es wird also jemand, der auch die Runentechnik beherrscht, den Text hier nicht direkt entnehmen können. Es sind verschiedene Entzifferungsversuche gemacht worden, aber bis heute ist man nicht sicher, welches die richtige Lösung darstellt.

Im"schwarzen Mittelalter", wie wir sagen, hat man Geheimschrift gleichgestellt mit Geheimtechnik, mit Alchimie und der Metaphysik, und hat alle Wissenschaften in einen Topf geworfen. Ein Abt Tritheim hat 1621 eine Anleitung über "Steganographie" veröffentlicht (Fig.4).



STEGANOGRAPHIA,
Hoc est:
ARS PER OC-
CVLTAM SCRIPTV-
RAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa,
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanheimensi, &
Magia Naturalis Magistro per-
fectissimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
vera introductio ab ipso Authore concinnata,
HACTENVS QVIDEM A MVLTIS MVLTVM DE-
siderata, sed à paucissimis visa.
Nunc verò in gratiam sectatorum Philosophiæ Studiosorum
publici iuris facta.
Cum Privilegio & consensu Superiorum.

DARMSTADII,
Ex Officina Typographica Balthasaris Aubrii, Sumptibus vero
IOANNIS BERNERI, Bibliop. Francof.
Anno M, DC.XXI.

Fig. 4

Steganographie ist die Art der "Versenkung" oder "Abdeckung" von Information in einem "vernünftigen" Text. An gewissen Plakatsäulen steht z.Zt. dieser Spruch zu lesen: "Zürich halte". Da ist den modernen Propagandaleuten wieder die Steganographie eingefallen, indem sie das "ich" hier in Zürich verpackt haben. Steganographie ist also die Art von "Verpackung" von Klartext in einen andern Klartext ohne irgend welche Veränderung, sie stellt also nicht eine direkte Chiffrierung dar, dient aber auch heute noch als wichtiges Geheimhaltungsmittel, überall dort, wo eigentliche chiffrierte Meldungen nicht übertragen werden können. Mikropunkte gehören z.B. auch in das Gebiet der Steganographie.

Wenn wir zu den Prinzipien kommen, die gültig sind für Schriftverschlüsselung, so heben sich zwei grundsätzliche Arten der Umstellung hervor. Die eine ist eine Versetzung der Textbuchstaben, auch "Transposition" genannt; als Beispiel diene die Skytale der Griechen. Das andere System ist die Ersetzung, d.h. jeder Buchstabe wird durch einen andern des Alphabetes ersetzt, eine Substutionsmethode wurde also erstmals von J.Cäsar vorgeschlagen.

Das sind die 2 Grundverfahren, die auch immer noch heute angewendet werden.

Sehr bald hat man festgestellt, dass ein Verschlüsseln von Hand mühsam ist und nach Hilfsmitteln gesucht; Fig.5 zeigt eine Rekonstruktion eines Hilfsgerätes von Baptista Alberti aus dem Jahr 1430, das allerdings nicht zur Verschlüsselung diente.

Fig. 5

Verschlüsselt wurde noch von Hand durch Umstellung; hingegen half das Gerät bei der Entschlüsselung. Es trägt zwei konzentrisch angeordnete Alphabetenringe und einen Zeiger, mit je 1 Fenster pro Ring, der die entsprechenden Referenzen gibt. Die beiden Ringe können gegeneinander verdreht werden. Aussen am Zeiger ist man dem Crypto-Buchstaben nachgegangen und hat im innern Fenster den entsprechenden Klarbuchstaben herausgelesen.

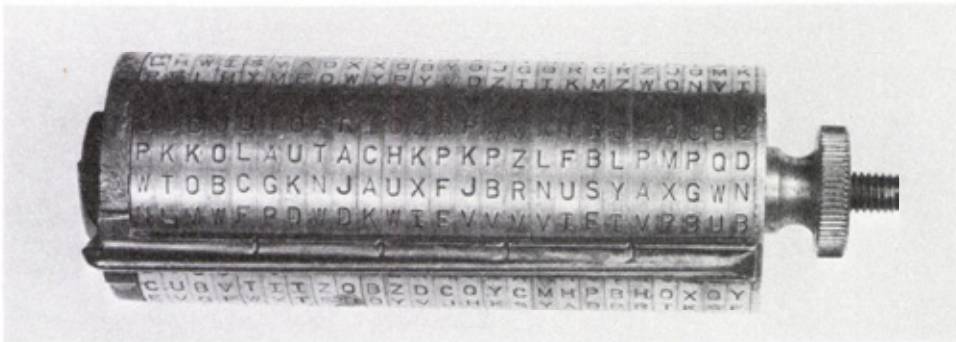


Fig. 6

Fig. 6 zeigt ein Hilfsmittel, das praktisch innerhalb eines Jahrhunderts zweimal erfunden worden ist. Zuerst durch Jefferson 1790 in den jungen Vereinigten Staaten und später, 1890 völlig unabhängig davon, von einem General Bazéries in Frankreich; sogar eine dritte Person scheint auch auf die gleiche Lösung gekommen zu sein. Dieses Ding, das sehr primitiv aussieht, ist im Koreakrieg von den Uno-Truppen, d.h. praktisch den Amerikanern, z.Teil noch verwendet worden. Es ist ein Stab mit einem Längskeil, auf welchem eine gegebene Anzahl zylindischer Scheiben sitzen, die Alphabete an der Peripherie tragen. Nach bestimmten Regeln werden die Zylinder aufgeschichtet und sitzen mit einer ihren 26 Nuten auf dem Keil des Zentralstabes, so dass sie nicht verdreht werden. An Hand des festen Lineals schichtet man die Scheiben für ein Stück Klartext auf den Stab und liest an einer andern zur Achse parallelen Stelle ab. Es ist also nicht ein Chiffriergerät, sondern ein Chiffrierhilfsmittel, im Prinzip eine aufgewickelte Chiffertabelle.

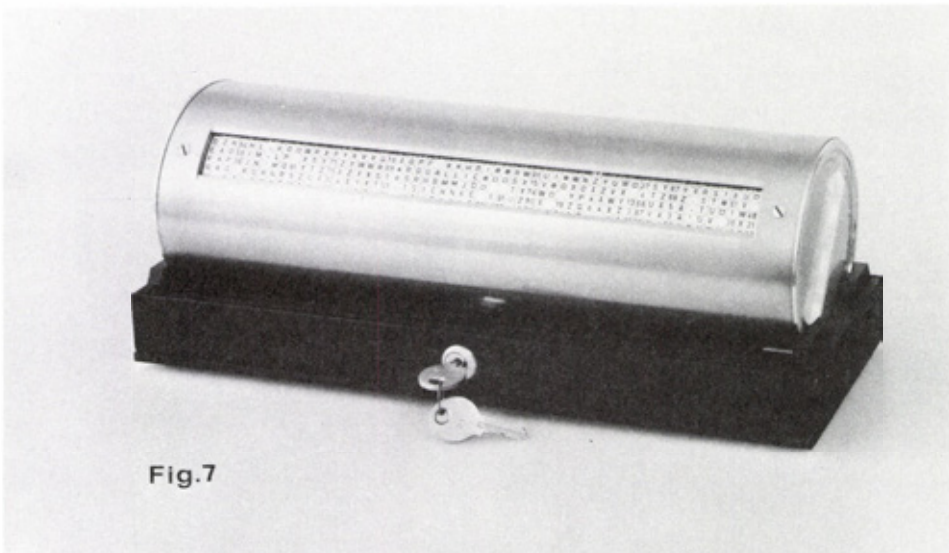


Fig.7

Fig.7 zeigt die erste eigentliche Chiffriermaschine. Es wurde weiter vorn auf den skandinavischen Boden hingewiesen. Nun, da war also ein Rittmeister Gripenstierna, der am 26. August 1786 seinem König Gustav dem III. eine Maschine abgeliefert hatte, wofür er untertänigst um 130 Reichskronen bat (Fig.8,9,10).

2-6

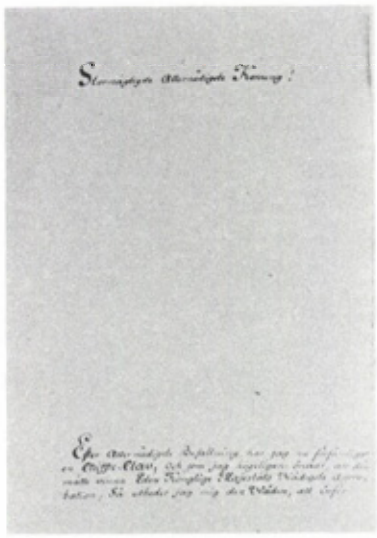


Fig. 8

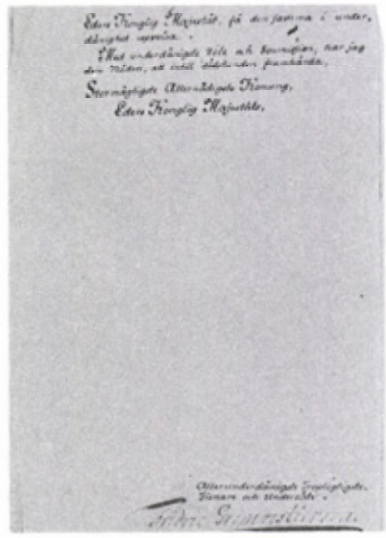


Fig. 9

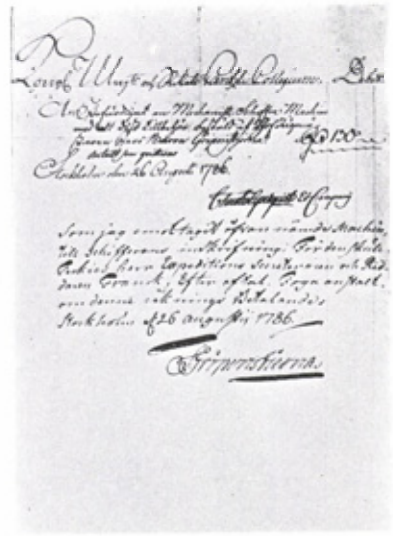


Fig. 10

Die Entdeckung, dass also bereits im 18.Jahrh. eine Maschine gebaut worden war, verdankt man den Forschungen, die seit ungefähr 15 Jahren in den Kriegsarchiven in Stockholm durchgeführt werden. Es liegen, ähnlich wie im Vatikan, viele Akten herum, die bisher noch nicht systematisch durchforstet wurden, und bestimmte Personen können auf Gesuch hin heute gewisse Dokumente untersuchen, allerdings sind auch heute noch namhafte, sehr alte Belege "tabu"!

Gripenstierna hat bereits die Grundidee gehabt, dass das Chiffrieren und das Schlüsseleinstellen voneinander zu trennen sind. Die Maschine war durch zwei Leute zu bedienen. Das Problem der "Gewaltentrennung" wie im Zivilleben von Gesetzgebern und Gesetzanwendern ist hier auch gleichgültig; derjenige, der sich mit dem Schlüssel herumschlägt, soll möglichst nicht wissen, was die Meldung enthält, und derjenige, der die Meldung verarbeitet, soll möglichst nicht wissen, nach welchem System die Verschlüsselung stattfindet (Fig.11).

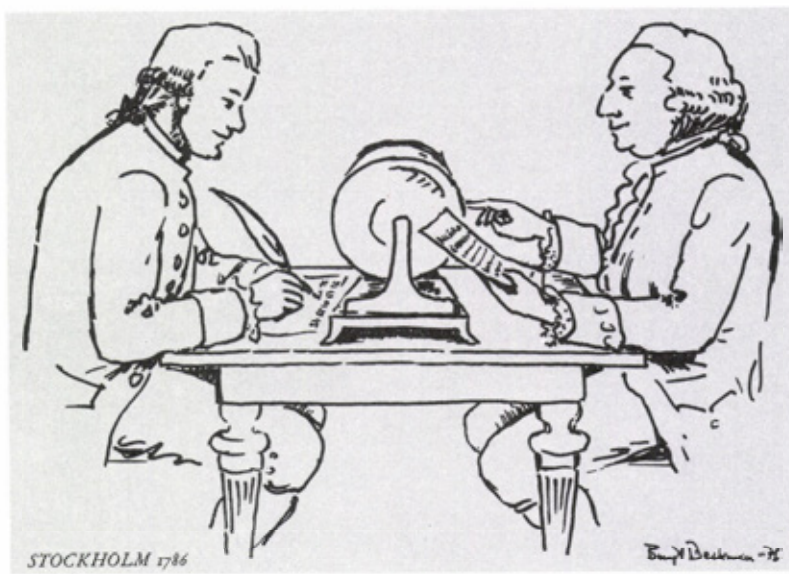


Fig. 11

Auf einer Seite wurde die Meldung verarbeitet, d.h. gegenüber fest angeordneten Buchstaben diejenigen im Fenster abgelesen, die auf den Peripherieen der Schlüsselräder graviert sind, und auf der andern Seite wurde der Schlüssel eingestellt, d.h. gegenüber fest angeordneten Zahlen die Schlüsselräder so verdreht, dass Zahlen an der Peripherie nach vorgeschriebener Schlüsselvorschrift sichtbar wurden.

Wie im 19.Jahrhundert die Telegraphie-Technik aufkam, ergab sich natürlich der Bedarf nach Verschlüsselungsgeräten mit entsprechender grösseren Kapazität für die Verarbeitung der Meldungen, und es ist logisch, dass die Leute, die sich mit der Telegraphie beschäftigten, sich auch mit Schlüsselfragen befasst haben.

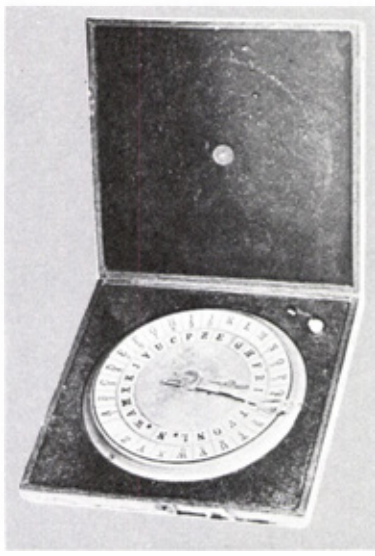


Fig.12

Auf Fig.12 wird eine Maschine von Wheatstone gezeigt, der u.a. die elektrische Widerstands-Messbrücke erfunden hat,und auch Vorschläge zu Buchstabentelegraphen ausarbeitete; Fig.12 ist übrigens das Bild eines Originalgerätes! Man erkennt zwei konzentrische Kreise mit Buchstaben und Ziffern, sowie zwei Uhrzeiger. Diese Uhrzeiger sind miteinander in einem Verhältnis zu 25:26 mechanisch gekoppelt und können mit Reibkupplungen gegeneinander in eine bestimmte Relativlage gebracht werden, was als "Startschlüssel" bezeichnet werden kann. Man kann z.B. annehmen, der grosse Zeiger stehe auf Z und der kleine auf Y, das sei die Startlage. Der grosse Zeiger wird nun immer gleichsinnig von Buchstabe zu Buchstabe eines Textes verdreht, der kleine Zeiger gibt dann einen Hinweis auf die zu verwendenden Substitutionsbuchstaben, die den Cryptotext bilden. Die Puristen der Mechanik werden sagen, "das stimmt ja mit der Teilung nicht". Nun, die Buchstaben-Felder sind so gross, dass das in der Praxis funktioniert. Für's Dechiffrieren wird umgekehrt vorgegangen: Man dreht den grossen Zeiger, bis der kleine Zeiger jeweilen auf dem richtigen Feld des zu verarbeitenden Cryptobuchstabens steht, und liest beim grossen Zeiger dann ab.

Fig.13 zeigt eines der Urgeräte aus dem "Crypto" Konzern, realisiert durch A.Damm. Die Gebrüder Damm waren beide geistig sehr aktive Leute und Arvid war enorm begabt für "Tüfteleien", (in einer technischen Hochschule geziehmt es sich eigentlich nicht zu reden von "Begabung", wenn es um Tüfteleien geht), für mechanische Sonderdinge, und er hat u.a. auch die Idee gehabt, Schlüsselmaschinen zu bauen, das im Jahre 1915! Die geniale Idee im ersten, richtigen Gerät, das er gebaut hat, liegt darin, dass der Schlüssel sehr leicht verändert und insbesondere rasch zerstört werden kann. Man erkennt eine Kette mit Gliedern, die zwei verschiedene Höhen aufweisen. Es gibt Glieder mit einem hohen Nocken und Glieder mit einem niederen Nocken. Weiter existiert ein Zylinder, der auf den Umfang in der Längsachse verschiedene verwürfelte Alphabete trägt, für jede Teilung des Zylinders eines. Der Zylinder wird bei Betätigung immer um eine Teilung verdreht. die Kette wird ebenfalls um ein Teilglied verschoben. Oberhalb des Kettenvorschubrads sitzt ein Fühler mit einer kleinen Rolle. An diesem Fühler hängt ein Bügel, der über die ganze Trommellänge hinweg geht und der ein lineares Alphabet, also A, B, C usw. bis Z, trägt. Je nachdem, ob ein hohes oder niederes

Kettenglied abgetastet wird, steht der Bügel oberhalb eines Zufallsalphabetes oder unterhalb eines solchen. Man wird also je nach Lage dieses Bügels das eine Alphabet oder das andere gegenüber dem Linearalphabet zu sehen bekommen, beim nächsten Schritt wieder eine neue Auswahl von zwei neuen Alphabeten. Die Kette wird logischerweise

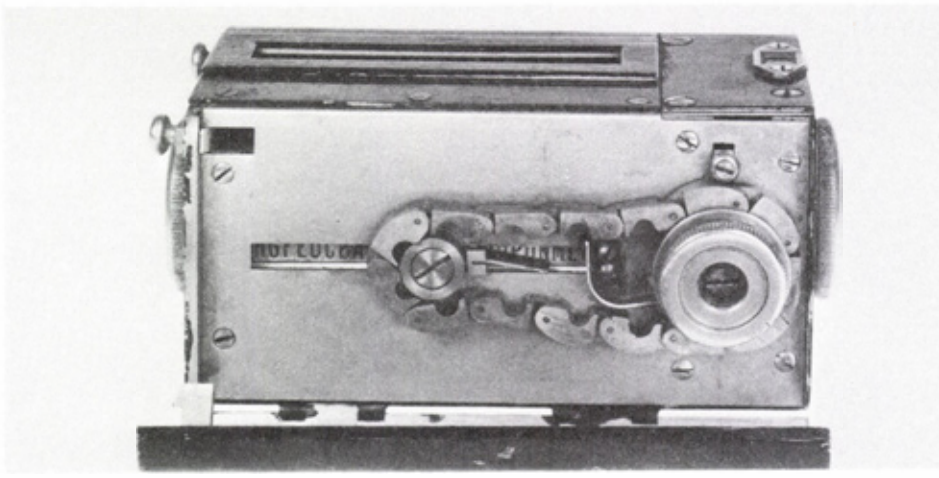


Fig. 13

mit einer Teilung versehen, die anders liegt als die Teilung der Trommel, beides möglichst Primzahlen, um grosse Perioden zu erreichen. Der Vorteil der Kette: wie erwähnt, kann diese sehr rasch auseinander genommen werden, d.h. sie zerfällt, wenn man das Gerät öffnet und senkrecht hält. Man kann auch auf einfache Weise die Kettenlänge verändern. Aus dieser Entwicklung heraus kam dann die nächste Maschine, die bereits in die Elektrotechnik ging.

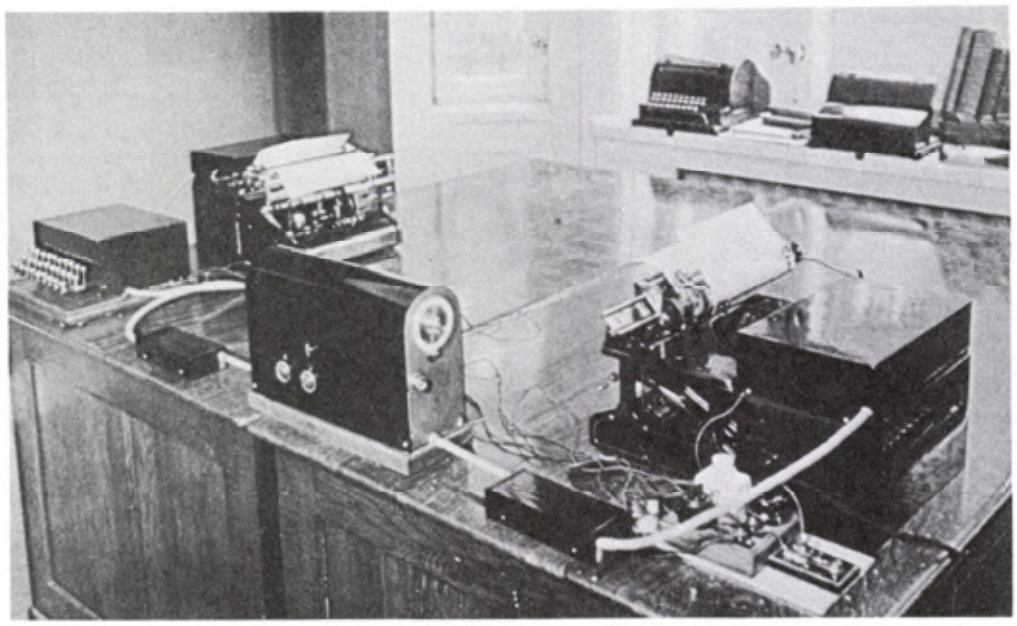


Fig. 14

Fig.14 zeigt eine grosse Kombination, die Herr Damm seinerzeit vorgesehen hat. Im Zentrum steht das "Herz" des eigentlichen Schlüsselmechanismus, hinten und vorn sieht man elektrische Schreibmaschinen, d.h. Maschinen, die elektrifiziert wurden (es gab dazumal noch keine elektrischen Schreibmaschinen), indem oberhalb des Tastaturfeldes ein Magnetraster angebaut wurde, der elektrisch die Tasten anschlagen lässt. Im Hintergrund links die Eingabetastatur, dazu ein Druckwerk für den Klartext und vorn rechts die Ausgabe. Das Gerät enthielt hier erstmals verwendete Durchgangsräder.

Fig. 15

Fig.15 zeigt eine Weiterentwicklung, die Boris C.W. Hagelin realisierte. Weiter oben wurde dargelegt, dass die Mechanik als Basis diente und A.Damm schon für die elektrische Verarbeitung mit der Tastaturmaschine Permutationsräder eingesetzt hatte. Das Ganze war aber sehr umfangreich, und wie in den 20er Jahren die "ENIGMA"-Maschinen in Deutschland auftauchten, interessierten sich auch die schwedischen Behörden dafür. B.Hagelin bat um ein wenig Zeit, er werde ihnen eine eigene Maschine machen! Das ist also der Urprototyp der Hagelin'schen B-211 Maschine (Fig.16), die später in grösserer Stückzahl auch in Frankreich in Lizenz gebaut wurde.

Fig.16

Dabei wurden vier Durchgangsräder und eine Eingabetastatur kombiniert. Zur Ausgabe dient eine der ersten Elektromatic-Maschinen, die "Remington Electric", die zu jener Zeit auf den Markt kam.

Die Durchgangsräder dienten zur Permutation von Kolonnen und Zeilen eines 5x5 Rasters (Fig.17). Wenn man eine Zeile und eine Kolonne mit einer Stromquelle verbindet, leuchtet die am Kreuzpunkt angebrachte Glühlampe auf. Wenn man die Kolonnenzuführung und die Zeilenzuführung vertauscht, wird im Feld die Lampensteuerung beeinflusst.

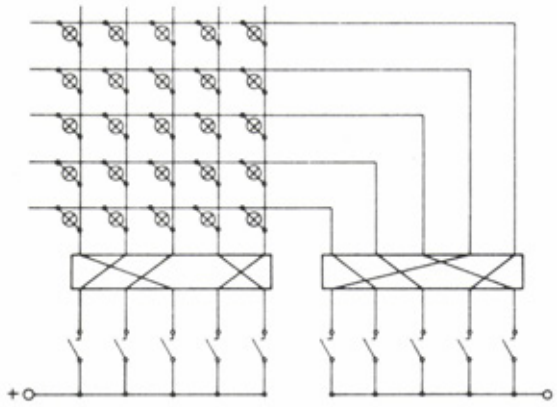


Fig. 17

Fig. 18

Fig.18 zeigt die Original-"ENIGMA". Diese Maschine ist plötzlich wieder aktuell geworden durch das Buch "Ultra Secret", nach welchem anscheinend die Alliierten seit 1938 diese Maschine kannten. Es wurde offenbar ein entsprechender Grossrechner gebaut, der, wie behauptet wird, alle Funksprüche der Achsenmächte während des Krieges mitlesen liess. Diese Maschine wurde gebaut durch Scherbius, der 1920 starb, (DRP 416 219), die Uridee kam aber vom Holländer Koch, der sie 1919 konzipiert hatte (NL Pat 10700), und 1919 hatte auch Damm die Durchgangsradidee, 1928 hat der Amerikaner Hebern ein Patent (US Pat.1'683'072) für eine Durchgangsrad-Maschine erhalten, dessen Idee aber 1918 schon realisiert worden war. Die Durchgangsradmaschine d.h. die elektrische Permutation zu Schlüsselzwecken, lag offenbar in der Luft zu dieser Zeit, und verschiedene Patente wurden unabhängig voneinander erteilt.

Die Mechanik war aber nach wie vor immer noch aktuell, weil ja die Mechanik hauptsächlich für den Einsatz im Feld unabhängig von einer Stromversorgung ist. Soweit ein Bedienungsmann noch seine Glieder benutzen kann, wird er auch ein Gerät mechanisch

betätigen können. B.Hagelin erhielt anfangs der 30er Jahre von den Franzosen den Auftrag, eine mechanische Maschine zu bauen, die in die "Tasche eines Waffenrockes" passen sollte, was er mit der C-35 auch schaffte (Fig.19).

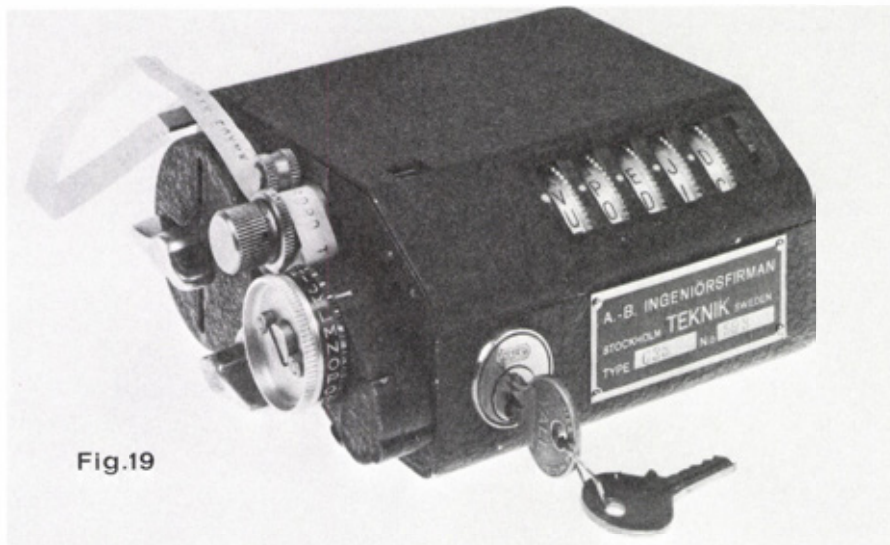


Fig.19

Aus der entstand dann die legendäre M-209 (Fig.20), die in den USA in 140'000 Exemplaren gebaut wurde.

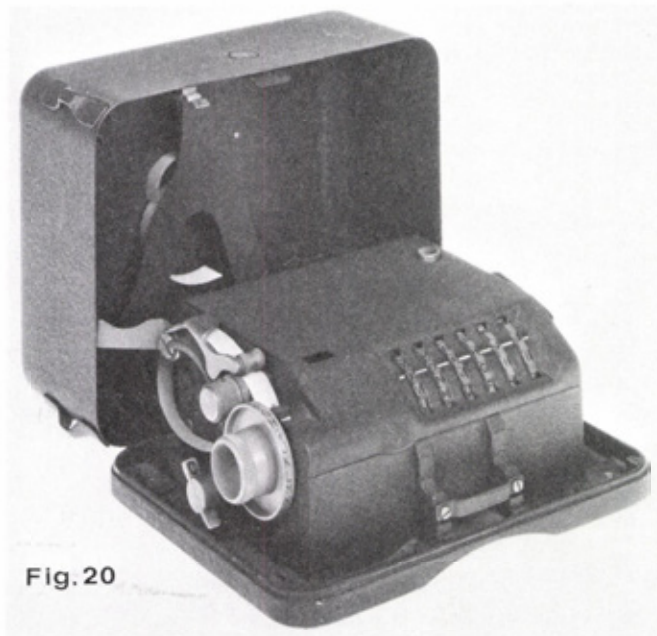


Fig.20

Es gibt wahrscheinlich kaum ein Gerät, das in dieser Stückzahl aufgetaucht ist. Dabei wurden in Frankreich kurz vor dem Krieg auch ansehnliche Stückzahlen C-36 in Lizenz gebaut, die mit der M-209 kompatibel sind. Aus dieser Maschine heraus kam dann eine Version mit Tastatur und Elektromechanik und zwei Druckwerken, wobei eine Kurbel ermöglicht, das Ding von Hand zu betreiben, falls einmal kein Strom da ist (Fig.21).

Fig. 21

Die Achsenmächte hatten natürlich ihrerseits auch Möglichkeiten entwickelt, in diese Maschine einzubrechen. Wenn man sich vorstellt, dass -zig Tausend Maschinen im Einsatz waren, so ist leicht zu erklären, dass hier der Faktor "Mensch" allerhand Unfug zur Folge hatte. Im Verlauf der Kriegsjahre wurden diese Maschinen, wie sie als Beutegeräte in Berlin auftauchten,von den Deutschen nachgebaut unter der Bezeichnung C-41. In den 30er Jahren hatte man vom neutralen Stockholm aus auch Berlin die C-35 angeboten. Sie war aber abgelehnt worden.

1941 bedeutete das Konzeptionsjahr, sie kam aber erst zu Einsatz Ende des Krieges, im Jahre 1944! Es wurden ca. 600 Stück gebaut, und in dem Moment wie diese Maschine zum Einsatz kam, ging bei den Alliierten offenbar "der Rolladen herunter". Sämtliche Funksprüche schienen dicht zu sein. Ein sonderbarer Fall, dass der Feind eine Maschine kopiert, die er ursprünglich als unbrauchbar abgelehnt hat, und diese dann so einsetzt, dass man selber dagegen nichts mehr anfangen kann. Die Deutschen hatten sämtliche Fehler und Schwächen des Systems der Alliierten kennengelernt, sie hatten erkannt, es sind überall nur die Menschen schuld, die Maschine ist gut, "der Beweis ist da". Sprüche dieser Maschine konnten von den Alliierten offenbar nicht geknackt werden.

Fig. 22

Allgemein ist zu merken: Die Chiffriermaschine ist generell das kleinste Glied in der ganzen Kette "Kommunikation". Alle andern Glieder sind fast wichtiger. Sie ist ein sehr wichtiges und angenehmes Hilfsmittel, aber sie ist das kleinste. Das Vorher und Nachher im ganzen Meldeablauf, die Einsatz-& Schlüsselbefehle sind das Wichtigste.

2. GESICHTSPUNKTE DES FABRIKANTEN

Die CRYPTO AG ist eine unabhängige Firma, die nur Schlüsselgeräte baut und von ihren Produkten leben muss. Es werden z.Zt. in rund 90 Ländern der Welt Apparate verkauft. Die Firma kann dabei nicht an eine Doktrin gebunden sein und muss schauen, allen Wünschen gerecht werden zu können, und das ist ziemlich kompliziert und mühsam. "Allen Leuten Recht getan ist eine Kunst, die niemand kann". Nun ist die Kryptologie fast wie eine Religion, und je nach Himmelsrichtung gelten andere Ansichten als richtig. Die CRYPTO hat auf Grund der 60-jährigen Erfahrung und der weltweiten Kontakte aber bisher mehr oder weniger geschickt beizeiten herausgefunden, was in der "Luft" liegt und was für Lösungen am besten realisiert werden können. Zum Glück ist es so, dass der grösste Teil der Kunden sich der Firma in Bezug auf das, was angeboten wird, anvertraut. Die meisten können gar nicht entscheiden, ob ein Gerät in Bezug auf die Kryptologie "gut" oder "schlecht" ist, und sie gehen davon aus, dass eine Firma, die einen weltweiten Kundenkreis hat, es sich nicht leisten kann, schlechte Produkte auf den Markt zu bringen!

Trotzdem seien einige Gesichtspunkte, die mit der Kryptologie als solcher im Detail nichts zu tun haben, aufgeführt, da sie Grundsätzliches betreffen. Sie sind in Tabelle A zusammengestellt. Eine weitere Stufe sind die kryptologischen Basisregeln. Man muss von einer Grundidee ausgehen damit man nicht verrückte Maschinen baut, die gar nicht eingesetzt werden können. Die Regeln sind in Tabelle B dargestellt.

- Die andere Seite kennt das Gerät, sie kennt es sehr gut, besser als der Erstgebraucher.
- Die andere Seite hat einige Klartexte und zugehörige Kryptogramme.
- Die andere Seite hat das gleiche Gerät für eigenen Einsatz auch im Betrieb, oder sie hat es zu Studienzwecken beschafft, legal oder auf andere Weise.
  Bsp.: SAM 7 1973
  MIG 25 1976
- Folgerung: Gerätemässige Geheimhaltung kommt nicht in Frage, Sicherheit muss im Programm (software) liegen.

Tab. A Grundsätzliche Gesichtspunkte

- Schlüssel soll mindestens so lang sein wie die Gerätelebensdauer.
  Bsp.: Uebertragungsgeschwindigkeit: 200 Baud
  Gerätelebensdauer: 25 Jahre
  Totalzahl der Zeichen: 10^{12}
- Kenntnis des Algorythmus soll Textanalyse nicht erlauben.
  Bsp.: Textlänge: 1000 Zeichen
  Analysegeschwindigkeit: 10^6 Analysen/sec, oder $3 \cdot 10^{13}$ Analysen/Jahr
  Gerätelebensdauer: 25 Jahre
  Totalzahl der Analysen: $25 \cdot 3 \cdot 10^{13}$
- Die obigen Kombinationen sollen in der gleichen Grössenordnung unwahrscheinlich sein.
  Periodenlänge: $10^{12} \cdot 25 \cdot 3 \cdot 10^{13} \cdot 10^{12}$ Zeichen, oder $\sim 10^{40}$ Zeichen
  (Vergleich: Alter des Universums: ca. 10^{18} sec)
- Aufteilung in Grund- und Tages- oder Meldungsschlüssel soll rein organisatorischer Art sein. Rangmässig soll kein Unterschied bestehen.

Tab. B Kryptologische Gesichtspunkte

Mann kommt also am Schluss ungefähr auf 10^{40} Zeichen für die Periode der Maschine. Das Wort "Periode" soll so verstanden sein, dass dies nicht eine gleichmässige Fortschaltung des Systemes betrifft, sondern die Anzahl Schritte, die das Gerät durchgehen muss, bevor es je wieder das gleiche produziert. Das Universum ist jedoch kaum 10^{18} Sekunden alt, wenn man von der Explosionstheorie ausgeht. Man erkennt die Grössenordnungen, mit denen man es hier zu tun hat!

Gerade so wichtig sind dann aber eben die kryptologisch vorgesehenen Abläufe innerhalb der Periode, auf die ich bewusst nicht eingehe. Das Spiel mit grossen Zahlen soll einen Verbraucher nicht blenden; es seien lediglich als selbstverständlich gültige Gesichtspunkte, eben die heute zu berücksichtigenden Grössenordnungen dargestellt.

Tab.C schliesslich gibt einige Grundideen wieder, die die Eingabe der Schlüssel oder Schlüsselprogramme betreffen.

1. Ab Klaviatur, eigen oder fremd.
2. Ab Tastatur (bei nicht schreibenden Geräten).
   Beste Lösung für Zweistufenschlüssel:
   Ganzer Schlüssel = X Gruppen; jede Gruppe einzeln veränderbar und leicht memorierbar.
3. Ab Lochstreifenabtaster.
   Ideallösung für Langzeitschlüssel; Software ist jederzeit in Hardwareform realisierbar, und die Hardware ist optimal zerstörbar.

Tab.C Eingabe der Schlüsselprogramme

Die dritte Version geht davon aus, dass in modernen Uebermittlungsystemen Fernschreiber ja meistens zur Verfügung stehen. Sollte das ausnahmsweise einmal nicht der Fall sein, so kann man handelsübliche Handstanzer, die wie Etiketten-Prägegeräte aussehen, benutzen, mit welchen man 5er oder 8er Lochstreifen für solche Zwecke in kurzer Zeit manuell herstellen kann. Lösung 2 ist für Zweistufen-Schlüssel. Wird die Programminformation in Gruppen aufgeteilt, so kann der Operateur bis zu einer 5er Zahlengruppe evt. ohne Niederschrift im Kopf memorieren und nach Instruktion eingeben, die übrige Schlüsselinformation (d.h. andere Gruppen) ist ihm nicht zugänglich und muss ihm auch nicht bekannt sein.

3. PRAXIS HEUTIGER GERAETE

In Fig.23 ist der Nachfolger der berühmten M-209 sichtbar, ein Vertreter der Maschinengruppe C-52, der gegenüber der früheren Version dicker und grösser geworden ist, wobei kryptologisch eine entsprechende Verbesserung erreicht wurde.

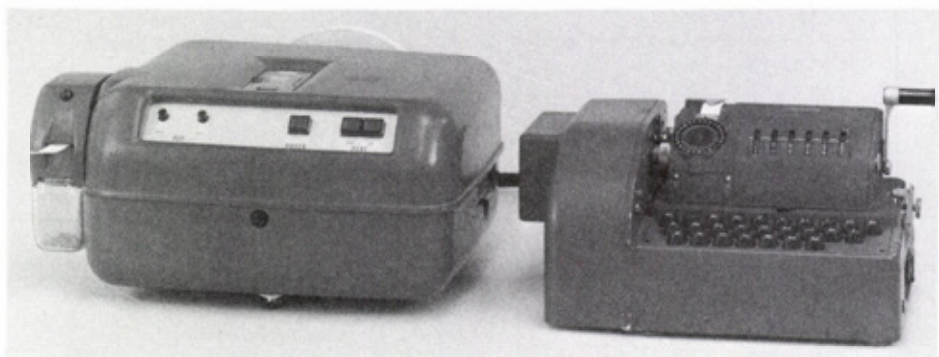


Fig. 23

Hier stehen grössere Primzahlteilungen der Stifträder zur Verfügung, die Stifträder sind austauschbar (total stehen 12 Teilungen zur Verfügung). Die Einstellung des Primärtextes geschieht anhand eines feststehenden Alphabetes und umlaufendem Zeiger. Es existieren davon keine 2 Varianten mehr wie bei der M-209 und der BC-543. Es ist lediglich ein einziges Gerät für den eigentlichen Verschlüsselungsvorgang vorhanden, in Fig.23 rechts sieht man, dass das Gerät auf einem "Traktor" sitzt, also einer elektrischen Klaviatur, die das Gerät antreibt. Bei Stromausfall kann das Gerät abgenommen und weiterhin als rein mechanisches System betrieben werden. Mit dem Tastaturuntersatz ist Betrieb ab 12V Batterie- oder einer der üblichen Netzwechselspannungen möglich. Links ist ein Zusatzgerät, das als "Brücke" zum Fernschreiber dient. Fernschreiber sind heute in den meisten Nachrichtenzentren vorhanden, oft wird aber vorgezogen, nicht einen direkten Fernschreibschlüsselverkehr im sogenannten "On-Line" Verfahren durchzuführen, sondern die Verschlüsselung und die Uebermittlung zu trennen.

Mit dem Zusatzgerät, dem PEB-61 ist es möglich, den primären d.h. den eingegebenen oder den sekundären d.h. den verarbeiteten Text auf Lochstreifen zu stanzen, wunschweise als endlose Buchstabenfolge oder aber in 5er Gruppen, 10 Gruppen zu einer Linie geordnet. Letzteres ist notwendig, falls in der Uebermittlungsstrecke irgendwo der Text in schriftlicher Form vorhanden sein muss. Findet eine Uebertragung direkt an eine Gegenstelle mit Fernschreiber statt, so wird logischerweise dort der Stanzer eingeschaltet und der entsprechende Kryptotext wird beim empfangenden Gerät in den Abtaster eingegeben. Man kann dann bei einem Gamellendeckel voll Kaffee zuschauen, wie der Entschlüsselungsvorgang automatisch abläuft.

Die Eingabe des Kryptotextes in einen Fernschreiber auf der Sendeseite und das Dechiffrieren auf der Empfangsseite sind ja eine der grössten Fehlerquellen beim Einsatz des Menschen als Zwischenstufe, da der Text nicht in Wortform, sondern Buchstabe für Buchstabe abgelesen und eingegeben werden muss. Wer das in der Praxis schon je unter erschwerten Bedingungen über längere Zeit durchführen musste, dem muss nicht erläutert werden, was für eine Sisiphus-Arbeit das darstellt. Der PEB-61 ist hier eine wahre Erleichterung und gleichzeitig ein Hilfsmittel zur Verbesserung der Uebertragungsqualität in der ganzen Meldungskette.

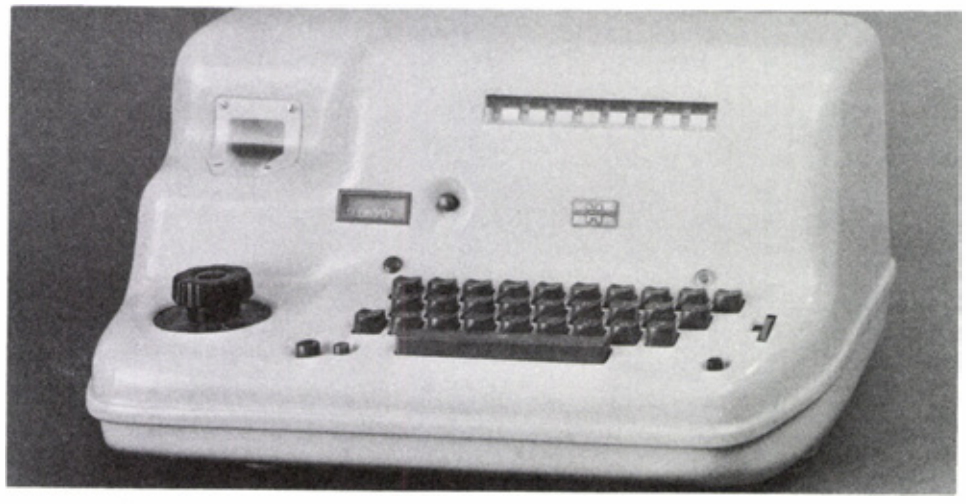


Fig. 24

Fig.24 zeigt wahrscheinlich den höchsten Entwicklungsgrad, der in der Elektromechanik erreicht wurde, man könnte fast sagen die Kreuzung eines Maulesels mit einem Zebra! In der Tat handelt es sich bei der HX-63 um ein Gerät, bei welchem die Ideen des unregelmässigen Stiftradvorschubes der C-52 Familie auf Permutationsrädern angewendet wurde. Es sind 9 vorhanden, deren gegenseitige Beeinflussung ebenfalls verstellbar sind. Die Anzahl der Durchgänge pro Rad ist höher als die Anzahl der zu verarbeitenden Schriftzeichen, wobei durch Rückführung eine mehrfach-Durchschlaufung der Information erfolgt, was kryptologisch von Vorteil ist.

Die Maschinengruppe C-52 (Fig.23), die rein mechanisch arbeitet, lässt verschiedenste Einstellmöglichkeiten zu. Schöpft man alle praktisch vernünftigen Einstellungen aus, so kommt man auf eine Zahl von rund $3x10^{124}$. Warum ging man auf solch umfangreiche Einstellmöglichkeiten los?

Bei mechanischen Geräten sind die Periodenlängen relativ kurz. Bei den C-52 Familien zirka 10^{11} bis ca 10^{12} Schritte. (Es sei dabei nicht vergessen: Universumsalter: 10^{18} sec. bzw. 10^{11} Jahre!)

Man sucht das Auftauchen phasengleicher Sprüche dadurch zu vermeiden, dass eben die Einstellungen häufig verändert werden. Phasengleiche Sprüche sind solche Meldungen, die zum Teil oder ganz mit gleichen Abschnitten aus einer gegebenen Schlüsselperiode verarbeitet wurden.

Will man sich diese enorme Zahl veranschaulichen, so sei als Beispiel folgender Vergleich vorgeschlagen:

Für jedes Gerät mit einer neuen Einstellung nehme man ein Sandkorn von 0,1 mm Kantenlänge. Beginnt man jede Einstellung Korn um Korn aufzuhäufen, so wird dieser Vortragssaal ziemlich rasch gefüllt sein, ja in Kürze wird der ganze Semperbau und schliesslich die volle Erdkugel durch Sandkörner ersetzt werden können. Hier hört es aber nicht auf, man kann weitere Behälter mit Sandkörnern füllen und kommt dann auf eine Grössenordnung von ca. 10^{81} Erdkugeln! Bei der HX-63 (Fig.24), wo wir mehr Räder, grössere Teilungen und dazu ja noch die verschiedensten Permutationsumstellmöglichkeiten besitzen, ergeben sich Zahlen von Einstellmöglichkeiten für die "astronomisch" ein zu kleiner Begriff darstellt. Nimmt man auch wieder nur die vernünftig anwendbaren Fälle, so kommt man auf eine Grössenordnung von 10^{600} verschiedenster Einstellmöglichkeiten, eine Zahl, die das menschliche Hirn überhaupt nicht mehr erfassen kann. Im seinerzeitigen Bestseller, das "Parkinson'sche Gesetz", wird dies ebenfalls dargestellt: ein Fahrradunterstand, der zu bauen ist und 2000 Franken kostet, wird im Verwaltungsrat stundenlang debattiert, ein neuer Flügel des Gebäudes zu 4 Millionen wird aber auf Vorschlag der Direktion innerhalb von 2 Minuten bewilligt. 2000 Franken sind ein Begriff, den der Mitteleuropäer noch einigermassen überblickt, 4 Millionen sind bereits eine Zahl, die als solche vom menschlichen Hirn nicht mehr erfasst werden kann.

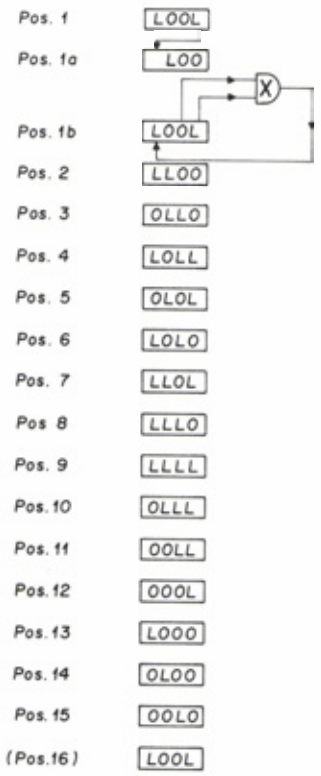
Fig. 25

Fig.25 zeigt ein Taschengerät der Serie CD-57, das mit Geräten der Gruppe C-52 kompatibel ist. Es besitzt kein Druckwerk, ist aber sehr praktisch und wird heute immer noch verlangt. Es sei hier vermerkt, dass die Geräte der Generation C-36 bzw. M-209 heute noch von verschiedenen Staatsorganisationen eingesetzt werden. Sofern die Einsatzvorschriften richtig befolgt werden, sind auch diese Geräte für bestimmte Fälle heute noch sicher wie je.

4. ARBEITSPRINZIPIEN MODERNER GERAETE

Moderne, elektronisch arbeitende Geräte sind rein digital organisiert. Dies ergibt sich daraus, dass heute Nachrichtenübertragungssysteme moderner Art ebenfalls digital arbeiten. Diese Lösung bietet den Vorteil, über beliebig grosse Distanzen hinweg mit Regenerationsstellen Meldungen fehlerfrei übertragen zu können. Fernschreiber- oder Dateninformationen sind als solche schon digital organisiert, auch Bildübertragungssysteme (Faximile). Für Sprachinformation wird an den Endstellen eine Umformung durchgeführt.

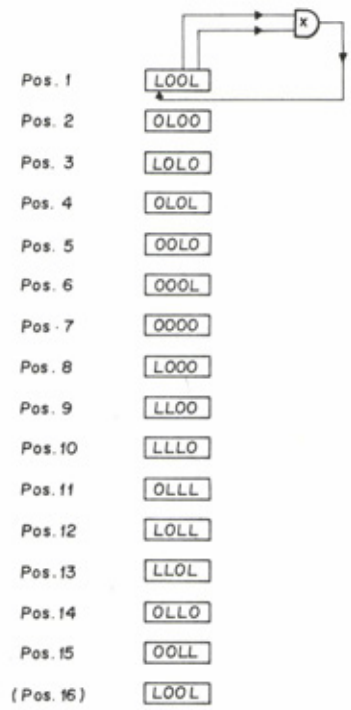
Wie erzeugt man nun in digital organisierten Systemen grosse Schlüsselzahlfolgen? Eine Lösung, die heute weltweit verwendet wird, liegt im rückgekoppelten Schieberegister.



Bildungsgesetz X :

O X L = L
L X O = L
L X L = O
O X O = O

Fig. 26



Bildungsgesetz x :

O x L = O
L x O = O
L x L = L
O x O = L

Fig. 27

In Fig.26 sei ein 4 zelliges Register dargestellt, bei welchem in Position 1 eine angenommene Füllung LOOL vorliegt. Ein solches Register besteht aus Kippstufen, die lediglich 2 Zustände einnehmen können. Sie können mit Röhren, mit Transistoren, ja auch mechanisch, hydraulisch bzw. pneumatisch realisiert werden. Die elektronische, heute übliche Version besteht aus integrierten Schaltkreisen, die alle notwendigen Elemente miteinschliessen.

Geht man auf diese Art weiter, so wird man nach 4 Schritten beim fünften wieder in die ursprüngliche Lage kommen, das Register verhält sich wie ein Rad mit vier Teilungen.

Wird nun aber in der Position 2 am linken, ersten Platz eine Information eingegeben, die nach Position 1b auf Grund eines Bildungsgesetzes, entsprechend der Darstellung unten im Bild erzeugt wurde, so ergibt sich eine viel längere Periode.

Aus Fig.26 ist ersichtlich, dass 15 verschiedene Zustände möglich sind und dass bei Position 16 wieder der gleiche Zustand wie bei Position 1 auftaucht. Das rückgekoppelte Schieberegister ermöglicht die Erzeugung von 2^n-1 verschiedener Füllzustände, wobei diese Zahl die maximale Möglichkeit darstellt, d.h. es sind sämtliche überhaupt möglichen Füllformen einmal vorhanden und zwar nur je ein einziges Mal. Dass die Anzahl Möglichkeiten nicht 2^n beträgt, ergibt sich daraus, dass die Trivialfüllung 0000 hier nicht vorkommt und auch nie vorkommen darf, da sie ja nach dem angewandten Bildungsgesetz keinen neuen Zustand zur Folge haben könnte, auch wenn ein Verschiebungsvorgang mit entsprechender Neufüllung technisch möglich ist.

Gewisse Veröffentlichungen behaupten nun aber, dass rückgekoppelte Schieberegister zur Erzeugung von Schlüsselketten unbrauchbar seien, da diese rekonstruierbar sind. Es ist natürlich einfach zu erkennen, dass ein solches Schieberegister wie ein Zähler abläuft. Bei einem Zähler wird man bei Position 13 leicht feststellen können, dass der nächste Schritt zu Position 14 führt, und dass vorher die Position 12 erreicht worden war. Aehnliche Ueberlegungen sind beim Schieberegister möglich. Für Schlüsselzwecke wird man also auf verschiedene Tricke zurückgreifen müssen, z.B. kann durch Kombinationen verschiedener Schieberegister eine Schlüsselkette erzeugt werden, bei der die Rekonstruktion eben nicht mehr möglich ist. Gleichzeitig wird die total zur Verfügung stehende Periode enorm vergrössert werden können.

Andere Möglichkeiten liegen in der Aenderung der Bildungsgesetze. Wird ein rückgekoppeltes Schieberegister, wie in Fig.27 dargestellt, durchgespielt, so ergeben sich wiederum 15 verschiedene Fälle. Die Reihenfolge ist aber eine andere als in Fig.26. Es ist ebenfalls ersichtlich, dass hier die Füllung LLLL nicht vorhanden ist, dafür die Füllung 0000. (Fig.27 siehe Seite 2-17)

Bei Registern grösserer Länge können die Abfragepunkte, bei denen Information zur Erzeugung einer Neufüllung abgenommen wird, an verschiedene Zellen angesetzt werden, allerdings muss man aufpassen, dass nicht Unterperioden entstehen. Es gelten nämlich ganz bestimmte Gesetze für die Auswahl derjenigen Abfragepunkte, deren Information, nach einem vorgegebenen Bildungsgesetz vereinigt, die Neuinformation darstellt, um eine maximale Periode zu erreichen.

Es ist also möglich, einerseits durch Kombination mehrerer Schieberegister extrem lange Schlüsselperioden zu erreichen, anderseits durch verschiedene, logische Vorgänge den Charakter verschiedenster Perioden, die unter sich gleich lang sein können, zu verändern. Es ist gezeigt worden, dass das Register aus Fig. 26 und das Register aus Fig.27, obwohl von der gleichen Startinformation ausgehend, total 15+15 verschiedene Zustände einnehmen können, theoretisch sind $15! \sim 10^{12}$ verschiedene Zustandsketten oder Alphabete möglich, allerdings sind nicht alle mit den einfachen Bildungsgesetzen wie in Fig.26 und 27 dargestellt realisierbar. Bei längeren Registern können aber entsprechende Grössenordnungen der Möglichkeiten erreicht werden.

Mann kann in modernen Geräten auch Mechanik simulieren, nach Fig.28 z.B. den Teil eines Alphabetringes, bei welchem am Umfang eine digitale Darstellung der zugehörigen Fernschreibcodeinformation aufgezeichnet ist. Die CRYPTO AG hat in den 60er Jahren solche Simulatoren hergestellt, die also auf elektronische Art mechanische Substitutionsvorgänge eines 26iger Systems nachbilden. Dabei wurden erstmals in Europa integrierte Schaltkreise eingesetzt. Es scheint, dass die Firma CRYPTO überhaupt die erste Firma auf dem europäischen Kontinent war, die diesen Schritt gewagt hat. Aufträge kamen von einem bestimmten Kunden, der für Meldezentralen rascher arbeitende Geräte wünschte, als die an den Aussenstellen eingesetzten elektromechanischen Apparaturen. (Fig.28 siehe Seite 2-19)

Eine andere Methode bedient sich der internen Umcodierung, wie dies im Winter 74/75 von Dr.Feistel schon erläutert wurde, und auf die Fig.29 kurz eingeht. Permutationen von 3 Plätzen zu 2 Zuständen geben theoretisch 24 verschiedene Fälle. Sind die Plätze mit dualer Information gefüllt, so ergeben sich in der Praxis aber nur 20 Fälle mit Wiederholungen. Wird eine Umformung des 3stelligen Dualcodes in die acht einzelnen Möglichkeiten durchgeführt und dann eine Permutation vorgenommen, so ergeben sich $8! = 4 \times 10^4$ Möglichkeiten. Im II. Weltkrieg wurde unter anderem der G-Schreiber bei den Achsenmächten eingesetzt, ein Fernschreiber mit eingeschlossenem Schlüsselteil, der den 5-plätzigen Dualcode des Fernschreibersystemes permutierte. Obwohl theoretisch 120 Möglichkeiten existieren, war der praktische Effekt nicht besonders überzeugend, wie aus dem eben Dargestellten entnommen werden kann.

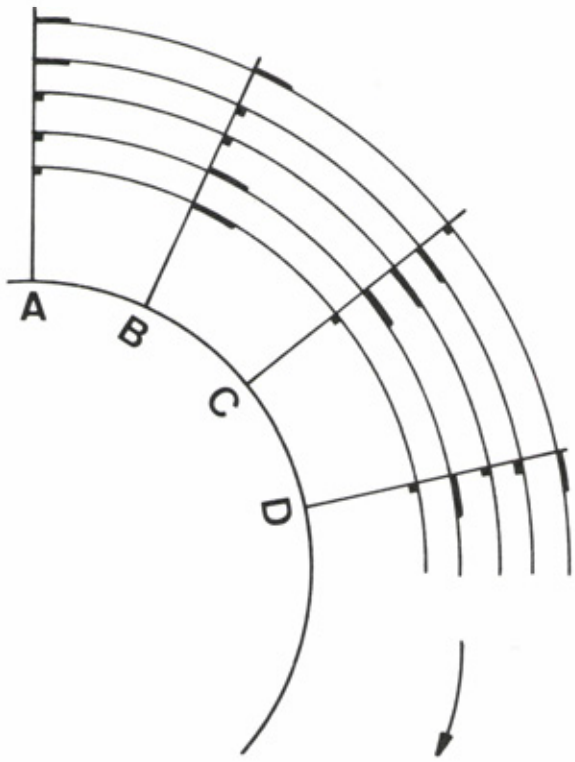
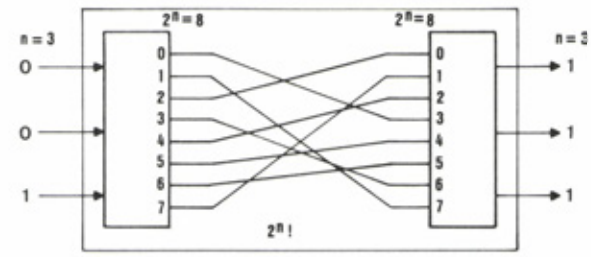


Fig. 28



3er Perm.: theoretisch $2^3 \cdot 3! = 8 \cdot 6 = 24$ Fälle

OOO			
OOL	→	OLO	LOO
OLO	→	LOO	OOL
OLL	→	LOL	LLO
LOO	→	OLO	OOL
LOL	→	OLL	LLO
LLO	→	LOL	OLL
LLL			

$8! \rightarrow 4 \cdot 10^4$

Fig. 29

Der Nachteil dieser Lösung, also Umcodierung mit anschliessender Permutation liegt, aber in der Realisation. Mit modernen elektronischen Mitteln ist es noch nicht möglich, auf einfache Weise sogenannte Durchgangsräder oder Permutatoren zu simulieren. Alle Verfahren sind sehr aufwendig, da sie digital arbeiten, und deshalb werden solche Verfahren selten eingesetzt. Ausserdem ist es nicht möglich, Fakultäts-zahlen und Zweier-Potenzen unter einen Hut zu bringen!

Man kann auch Folgendes machen: man kann die Codeumformung so darstellen, dass man homonyme Zuteilungen macht, das Wort Chiffrieren kommt ja von den Zahlen und die erste Chiffriertechnik, die diesen Namen verdient, war eine Umschreibung der Buchstaben mit Zahlenbigrammen, man kann für das A den Stellenwert im Alphabet nehmen und die nächsten Stellenwerte um Alphabetlänge verlängern, wie in Fig.30 dargestellt. Dann hat man für jeden Buchstaben 3, 4 oder 5 verschiedene Zahlen. Das erhöht auch die Möglichkeit, eine Verschlüsselung auf digitale Weise zu vergrössern. (Fig.30 siehe Seite 2-20)

Schliesslich gibt es die Möglichkeit, eine textabhängige autoklave Verschlüsselung durchzuführen. Herr Hagelin hat im Jahre 1943 eine mechanische autoklave Maschine gebaut. Es ist ein Gerät, das den Schlüssel fortwährend selber vom Text abhängig erzeugt, das ist auf den ersten Blick gesehen die ideale Lösung! Es wären überhaupt keine Angriffspunkte da für jemanden, der einbrechen will! Aber für den praktischen Fall ist das katastrophal. Die Uebertragung kann ja nie fehlerlos stattfinden, und wenn ein Zeichen falsch angekommen ist, ist der ganze Rest unbrauchbar. Man kann also autoklave Geräte wohl bauen, kann sie aber in der Praxis nicht einsetzen. Allerdings sind heute Teil-Autoklaven-Systeme realisierbar und anhand von Fig.31 sei, als ganz primitives Beispiel ein Vorschlag erläutert, wie so etwas möglich ist.

A = 01 & 27 & 53 & 79
B = 02 & 28 & 54 & 80
C = 03 & 29 & 55 & 81
D = 04 & 30 & 56 & 82
ETC.

Fig. 30

L + L = 0
L + 0 = L
0 + L = L
0 + 0 = 0

L + L = 0
L + 0 = 0
0 + L = 0
0 + 0 = L

Fig. 31

Weiter vorn wurde dargelegt, dass man beim Schieberegister die Bildungsgesetze verändern kann. Man kann auch beim Verschlüsseln die vordere Kolonne aus Fig.31 als die Klarinformation, die zweite Kolonne als die Schlüsselinformation werten und die 3. Kolonne als den Kryptotext. Macht man jetzt bei jedem fortlaufenden Schritt eine textabhängige Entscheidung, z.B. wie folgt: ist die vorhergehende Information eine Eins, so soll für den nächsten Chiffriervorgang die Gruppe Fig.31 a) gelten, und wenn es eine Null war, soll die Gruppe Fig.31 b) gelten. Man greift also in die 2. Kolonne nicht ein, sie ist gegeben, und wird erzeugt durch die sogenannten Schlüsselgeneratoren, die synchron an beiden Enden laufen, aber der Schlüsselvorgang als solcher wird beeinflusst und zwar vom Text.

Hier also ein ganz primitiver Vorschlag, man wird gebeten zu glauben, dass solche Geräte nicht gebaut werden! Das diene nur als Hinweis, wie z.B. der Einfluss auf den Schlüsselvorgang durch den Text selber gesteuert werden kann.

5. MODERNE OFF-LINE GERAETE

Aus der Praxis nun einige Beispiele von reellen Geräten: Fig.32 zeigt eine Maschine, die vollelektronisch verschlüsselt.

Fig 32

Nachdem es sich ja um eine Buchstabenmaschine handelt, braucht man logischerweise eine Eingabetastatur sowie ein Druckwerk. Aus der Tradition heraus ist sie jedoch als Zwillingsdrucker ausgelegt, so dass der primäre und der sekundäre Text immer vorhanden sind, was für den Operateur sehr von Vorteil ist, falls er gestört wird. Er kann immer sofort rekonstruieren, wo im Text er stand, ob er jetzt Ver- oder Entschlüsselung vornahm. Rechts eine kleine Befehlstastatur für Klartext, Chiffrieren, Dechiffrieren, Eingabe des externen Schlüssels (Meldungs- oder Tagesschlüssel) und Eingabe des internen Schlüssel (Grundschlüssel).

Die Taste zur Eingabe des internen Schlüssels ist mit einem mechanischen Schloss verriegelt, das nur dem Vorgesetzten der Chiffrierorganisation zugänglich ist. Der Operateur hat überhaupt nichts mehr zu öffnen, er hat nur noch seinen externen Schlüssel einzugeben, dazu drückt er Taste "E" und gibt auf der Klaviatur eine 5er Gruppe ein, entweder nach der klassischen Weise ab Tabellen, die geheim sind, oder - wieder ein Vorteil der modernen Elektronik - indem er sich selber eine Zufallsfolge macht.

Der Tagesschlüssel ist heute nicht mehr unbedingt geheim zu halten, weil er im Prinzip nichts darstellt, als einen Zählerstand auf der enorm grossen Periode des Gerätes. Nimmt man diese z.B. der Einfachheit halber als Uhr an, so sagt der Meldungsschlüssel: "ich steige auf das "Karussel" bei 2 Uhr ein" oder "um 16 h 17 und 10 Sekunden", oder "ich steige bei 2301 ein". Der Spruchschlüssel ist also nur noch eine Meldung, wo in der enorm grossen Periode (wie weiter vorn erläutert: Grössenordnung 10^{40} Schritte) einzusteigen ist. Das empfangende Gerät kennt diesen Punkt und wird sich entsprechend einstellen. Bei mechanischen Geräten hätte das geheissen: "Durchkurbeln und auf 10^{x} stellen". Das ist praktisch unmöglich. Bei der Elektronik kann man aber in der Sekante durch den Periodenkreis hindurchfahren, ohne dass man sämtliche Phasen durchspielen muss! Der Spruchschlüssel wird also am Kopf der Meldung mitübertragen.

Allerdings wird er nicht tel-quel im Gerät ausgewertet. Das Gerät verschlüsselt die eingegebene Spruchschlüsselinformation mit dem vorhandenen Grundschlüssel und das somit errechnete Resultat bildet die eigentliche Startstelle.

Sie ist somit als solche also keinem Menschen bekannt. Nur Geräte, die mit gleichen Grundschlüsseln programmiert sind, können den Einsatzpunkt errechnen.

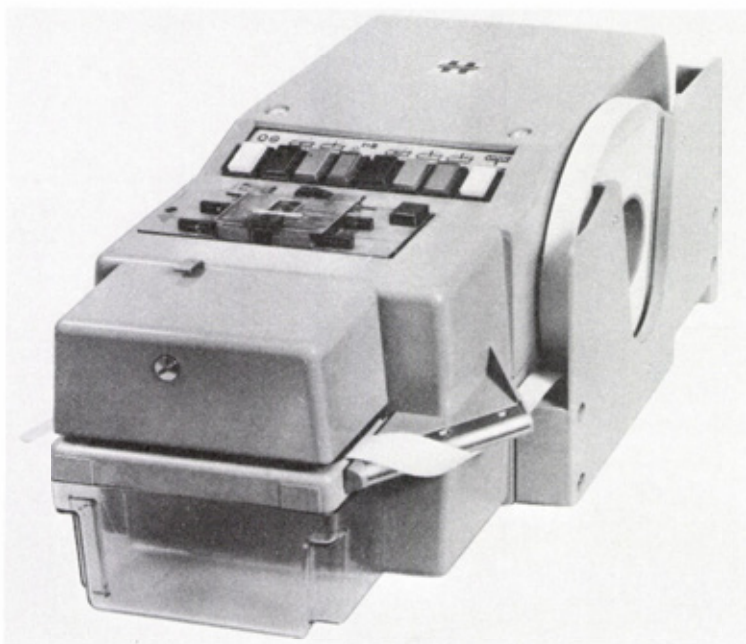


Fig. 33

Fig.33 zeigt wieder ein Zusatzgerät (PEH-72) analog dem PEB-61 (Fig.23), womit man auch wieder einen Fernschreiberlochstreifen erzeugen oder einen solchen Streifen auswerten kann. Es bietet auch noch die Möglichkeit (das ist auch beim PEB-61 der Fall), dass vom entschlüsselten Text, der ja klar, aber GEHEIM klassifiziert ist (und somit wohl meist mindestens in zehn Exemplaren gestempelt verteilt werden muss!), automatisch Blattkopien erstellt werden können. (Nach dem Parkinson'schen Gesetz ist es ja üblich, Geheimakten mindestens in 10 Exemplaren zu erzeugen, da muss man also Kopien davon machen.) Man kriegt vom Gerät aber nur einen Telegraphenstreifen. Wie macht man Kopien? Abschreiben gibt Fehler, das einzige Vorgehen ist folgendes: Streifen mühselig auf Blätter kleben und nachher Photokopien machen.

Falls nun aber ein Fernschreiber im Haus steht, kann man ihn ja als elektrische Schreibmaschine "missbrauchen". Die PEB-61 und PEH-72 können vom Dechiffrat auch einen Lochstreifen erzeugen, diesen schiebt man in den Abtaster des Fernschreibers, und der erzeugt beliebig viele Kopien und zwar Blattkopien, nur muss man dafür sorgen, dass die Uebertragungsleitung vorher abgehängt wird!

Fig. 34

Fig 34 zeigt ein Gerät aus Oesterreich (einige Zuhörer werden geglaubt haben, ein schweizerisches Gerät zu erkennen; es dürfte aber jenem "nachempfunden"sein). Es enthält einen Streifen-Drucker, eine Buchstabentastatur und einen Wanderschrift-schirm für die Primärdarstellung. Hier wurde also auch an den Operateur gedacht. Den Primärtext hat er stets stückweise vor sich; wenn er gestört wird, weiss er, wo er stand.

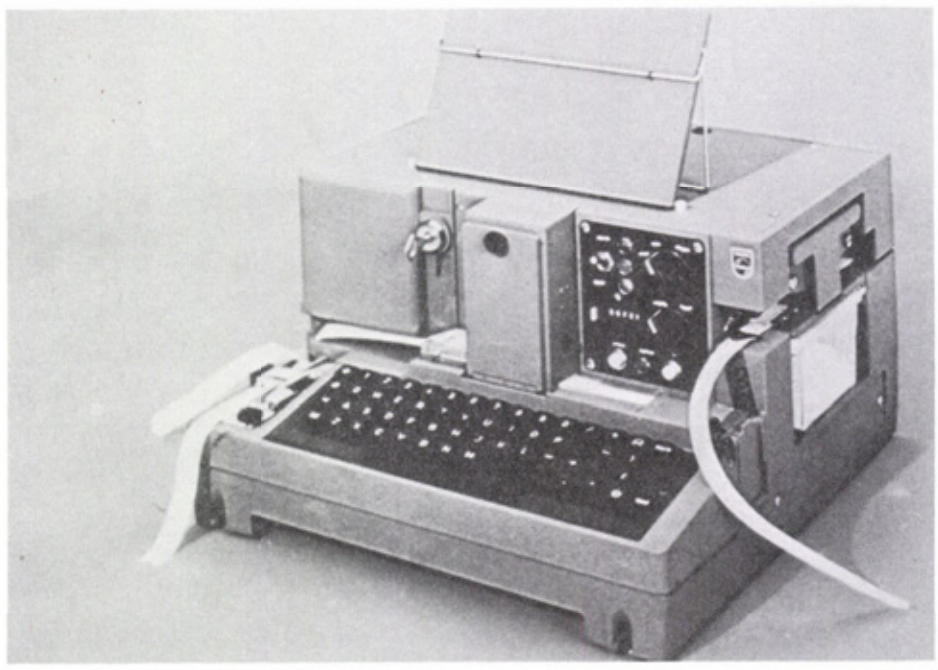


Fig. 35

In Fig.35 ist ein Gerät aus Schweden zu sehen. Das Gerät ist elektromechanisch konzipiert. Die Behörden dieses Landes haben gleiche Zeitkonstanten wie bei uns. Der Waffenchef hat in seiner Ausführung vor vierzehn Tagen erläutert, dass es in der Schweiz ungefähr 10 Jahre dauert, bis etwas zur Truppe kommt. Hier ist die Einführungszeit noch grösser gewesen: am Schluss wollte man selber etwas bauen, und heute möchten alle lieber ein modernes Gerät statt solch einer "Dreschmaschine" Es sind ungefähr vier Achsen drin, über Riemen und Zahnräder miteinander gekoppelt, wobei aber der Chiffriervorgang vollelektronisch durchgeführt wird. Die ganze Mechanik ist nur notwendiges "Zubehör", um den Stanzer, den Drucker und den Abtaster anzutreiben! (Nebenbei gesagt: die CRYPTO AG hat hier auch die Finger im Spiel!)

Fig.36

Was Technik heute bieten kann, zeigt Fig.36. Ein alphanumerischer Blattschreiber mit einem Wanderschriftschirm für den Primärtext (eine halbe Zeile lang) mit Thermodrucker, Streifenstanzer (beide für 30 Zeichen pro Sekunde) und einem optischen Abtaster für Lochstreifen. Alles in einem Gerät kombiniert. 7 gespeicherte Grundschlüssel, textabhängige Schlüsselung, weitgehende Automatisierung der Ablaufsequenzen. Falls man sich den Text im Hotelzimmer vorbereiten kann und ihn nicht gern an der Reception dem Telexfräulein geben will, kann man seine Telephonstation nehmen und nach Hause anrufen, hinten einen Telephonkoppler anstecken und den Lochstreifen schnell durchlaufen lassen. Die Uebertragung erfolgt dabei gesichert, indem im System eine ARQ-Anlage für Zweitontelegraphie mit eingeschlossen ist.

Das Gerät arbeitet mit einem Mikroprozessor. Das ist das moderne "Zauberding", worüber heute alle Welt spricht. Mikroprozessoren sind heute "en vogue" in Nähmaschinen, in Waschmaschinen, in Verkehrssteueranlagen, ja es gibt schliesslich auch Computer, die Mikroprozessoren enthalten, dafür wurden sie ja eigentlich entwickelt.

Fig. 37

Weiter vorn wurde auf die Möglichkeit elektronischer Taschenmaschinen verwiesen; Fig.37 gibt ein Bild davon. Man denke bitte beim Begriff "Tasche" an den Waffenrock. Es ist also noch nicht ein zündholzschachtelgrosser Minirechner, wie die "Casio" sie ver-

kauft, sondern es ist ein Gerät, das als Kompromisslösung für die Praxis entwickelt wurde.

Die CRYPTO AG muss rund 90 verschiedene Himmelsrichtungen oder Länder beachten! Die Bedingungen sind gegeben; einmal mit der alphanumerischen Tastatur, die der Operateur möglichst nicht mit dem Kugelschreiber antippen sollte, sondern von Hand, da er nämlich den Kugelschreiber für die Niederschrift braucht. Dann ein Wanderschriftschirm in Form eines alphanumerischen Anzeigefeldes mit Flüssigkristallen (damit die Batterie nicht jede Stunde ausgewechselt werden muss), dies gibt auch eine bestimmte Mindestgrösse. Die Tastatur ist übrigens eine Eigenentwicklung der CRYPTO, es gab bisher auf dem Markt noch keine staubdichte Tastatur. Es wurden ungefähr 50 Fabrikanten von Taschenrechner-Tastaturen angefragt, keiner hat etwas anbieten können, und so musste eine eigene entwickelt werden. (Sie wurden übrigens in erster Linie für die Sprachschlüsselgeräte gebaut und nachher für die HC-520 erweitert). Die Maschine HC-520 (Fig.37) ist übrigens kompatibel mit der CRYPTOMATIC HC-570 (Fig.36). Man kann also in den Aussenposten mit dem Gerät HC-520 arbeiten und auf der Zentrale die HC-570 einsetzen.

Fig. 38

Einen andern Lösungsvorschlag zeigt Fig.38. Auf den ersten Blick scheint das Gerät sehr elegant, es weist wohl eine alphanumerische Tastatur und eine Anzeige auf. Aber der Kryptotext besteht aus Ziffern, für jeden Buchstaben ein Ziffernpaar! Die Leute, die das übermitteln und rückarbeiten müssen, sind nicht besonders zu beneiden.

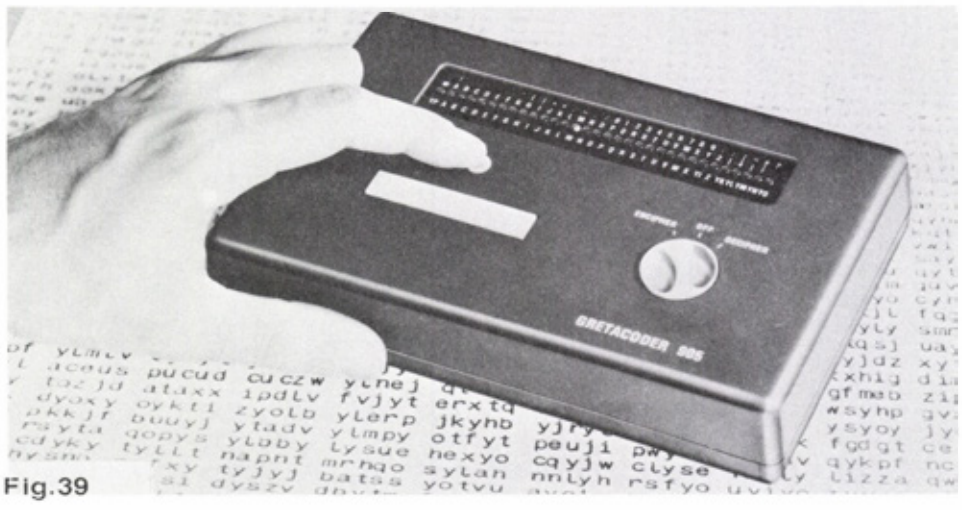


Fig.39

Fig.39 (siehe vorangehende Seite) zeigt auch eine elegante Lösung. Man nimmt ein stillstehendes Alphabet und lässt einen Zeiger - das ist heute eine Lichtmarke - daran vorbeilaufen. Der Vorteil: man hat kein Problem mit nicht-lateinischen Alphabeten. Man kann hier irgend eine Buchstabenfolge aufkleben, sei es ein Zufallsalphabet oder ein arabisches oder ein chinesisches, kurz irgendeines, das mit 26 Buchstaben auskommt oder mit vielfachen von 26, wenn man noch "Umschaltzeichen" dazu wählt. Aufpassen muss man allerdings enorm, dass einem beim Verarbeiten von Text Primär- und Sekundärbuchstaben nicht durcheinander geraten, man sieht ja stets nur eine einzelne Anzeige.

Dies waren einige Beispiele moderner Geräte für alphanumerische Zeichen, alles Geräte, die unabhängig von der Uebermittlung arbeiten, sogenannte "off-line" Geräte. (Die Lochstreifenzusätze ergeben keine direkten on-line Geräte, sondern bieten die Möglichkeit, ein off-line Gerät in den Fernschreiberkreis einzubeziehen.)

6. ON-LINE GERAETE

Natürlich hatte A.Damm um 1918 auch schon an dem Problem herumgeübt, zu der Zeit kannte man hauptsächlich die Morsetelegraphie, Creed England fabrizierte bereits tastaturbetriebene Locher für Streifen, die mit Automaten dann Morsecode aussendeten. Auch Umsetzer gab es von Creed, die in Morse eingegebene Information in Klarschrift ausdrucken.

Verschiedene Patente für Schlüsselgeräte, kombiniert mit Creed'schen Morsemaschinen wurden angemeldet, zu einer richtigen Entwicklung kam es aber nie. Der Morsetelegraph war ein Ding, das von Amt zu Amt lief, sofern es sich um den zivilen Sektor handelte, und bei der jungen drahtlosen Telegraphie war die Fehlerrate für automatischen Betrieb noch zu gross.

Herr Hebern, der 1918 in Amerika eine Durchgangsmaschine konzipiert hatte, hat natürlich weiter gearbeitet und im II. Weltkrieg wurden Hebern-Maschinen von der Western-Electric Gesellschaft mit Fernschreibern für on-line Betrieb kombiniert, wie ja anderseits Deutschland den G-Schreiber zum Einsatz brachte, wie weiter vorn erläutert.

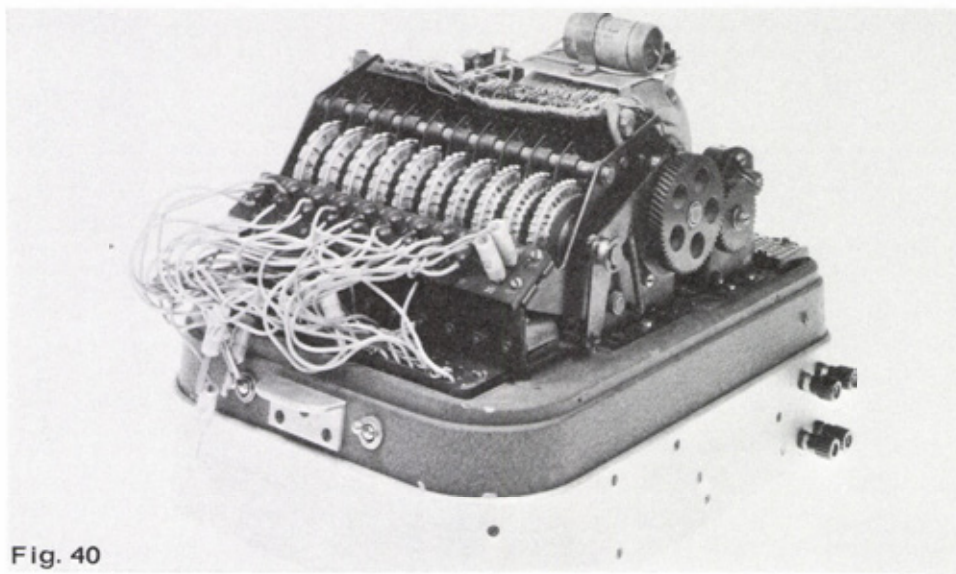


Fig. 40

Fig.40 zeigt eine Entwicklung,in Stockholm begonnen, die später in Zürich noch mit einem Anhängsel versehen wurde. Es ist dies der Vorläufer der TC-5 on-line Geräte und ihrer Nachfolger. Das Gerät konnte sowohl für den 5-stelligen internationalen Fernschreibcode wie für einen speziellen "5 aus 14" Code eingesetzt werden.

Fig.41 zeigt ein Gerät, das dem obigen stark "nachempfunden" zu sein scheint!

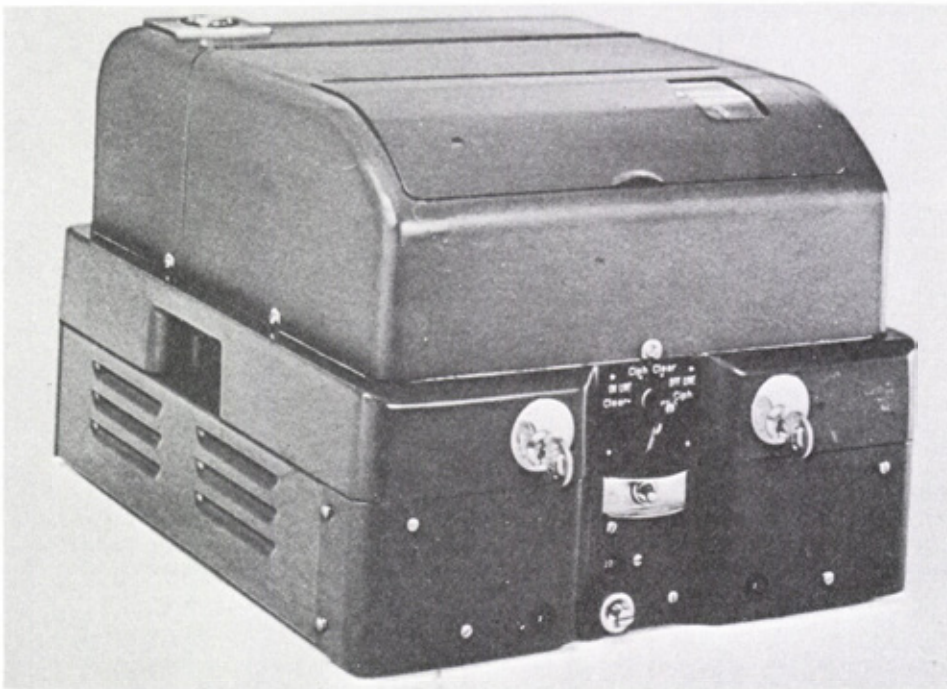


Fig. 41

Fig.42 zeigt das heute weltweit im Einsatz stehende T-450, die CRYPTROL, ein on-line Schlüsselgerät für Fernschreibbetrieb bis zu 100 Baud, Schlüsseleingabe ab Fernschreiber (Der Grundschlüssel ist dabei als einziger geheim). Der Operateur hat mit dem Chiffrieren nichts mehr zu tun. Er gibt nach Betriebsaufnahme ab Tastatur den Textbefehl für Cryptobetrieb ein, worauf ein Meldungsschlüssel automatisch eingegeben und gesichert übermittelt wird. (Für Systeme "alter Schule" ist Spruchschlüsseleingabe ab Tabelle auch möglich!) Wie weiter vorn erläutert, ist der Meldungsschlüssel ja nicht mehr geheim, sondern stellt nur einen "Zählerstand" dar. Aber damit einer, der zufälligerweise mithört, damit nichts anfangen kann, wird dieser "Zählerstand" mit dem Grundschlüssel, der schon im Gerät steckt, überschlüsselt und geht in dieser Form in das Rechenwerk ein. Man braucht also unbedingt physisch ein so programmiertes Gerät, wenn man auf der Leitung als "Datenklau" etwas vernünftiges anfangen will. Ein Gerät physisch zu stehlen, verursacht aber schon allerhand Wirbel, wenn es entdeckt wird, was in einem normal bewachten Netz rasch der Fall ist. Ohne programmiertes Gerät kann aber der liebe Gegner nichts anfangen.

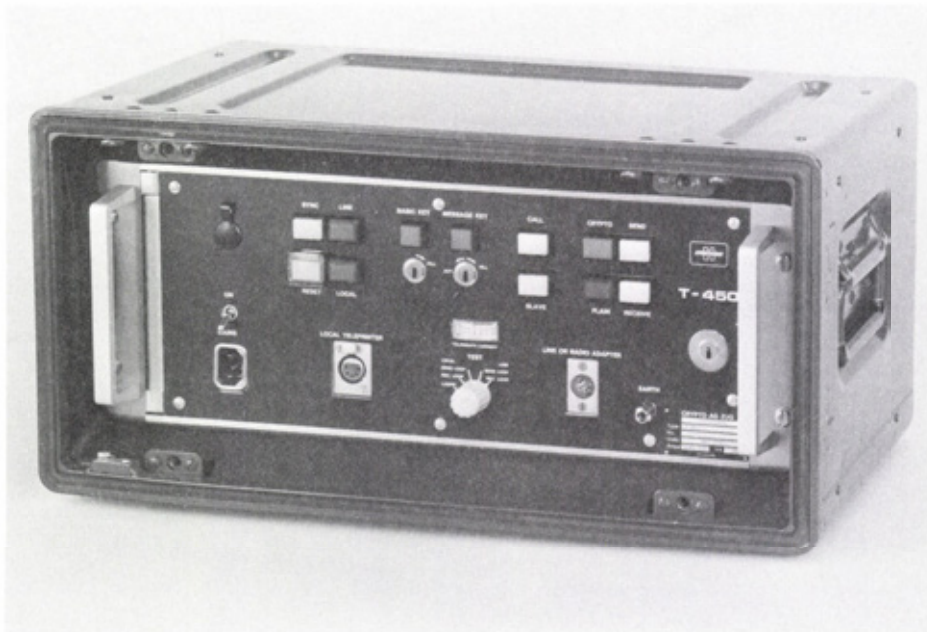


Fig. 42

Fig.43 zeigt die zivile Version des gleichen Gerätes. Das T-450 kann übrigens über irgend welche Fernschreiberverbindungen arbeiten, Start-Stop oder Synchron, über Feldleitungen, Satellitenleitungen, Abruf-Leitungen, Funkstrecken etc. An einem Stecker kann der Abruf-takt eingegeben werden für Systeme, die extern gesteuert werden.

Fig. 43

Fig.44 zeigt ein Gerät, das ungefähr gleiche Funktionen ausübt wie die T-450, aber für einen beschränkten Kundenkreis mit bestimmten Vorstellungen entwickelt wurde, somit weniger universell einsetzbar ist.

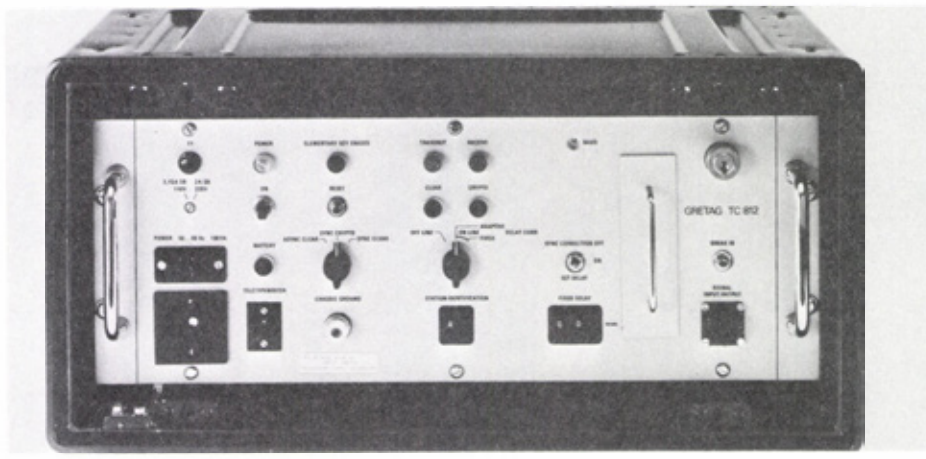


Fig. 44

Fig.45 zeigt eine Version aus USA, die offenbar der Zivilversion der T-450 "nachempfunden" wurde. Die erhältlichen Informationen erzählen von einigen "zig-milliarden" Kombinationen. Es ist immer etwas verdächtig, wenn Leute sich mit Milliarden und Billionen herumschlagen! Es wurde einmal im "Electronics" ein 2-seitiger Artikel über das Gebiet veröffentlicht, und am Schluss stand: ein Telephongespräch mit der CRYPTO habe ergeben, dass ihre Geräte nur ca. 10^{100} Einstell-Möglichkeiten zuliessen, weiter vorn im Artikel wurden andere Geräte erläutert und dabei war von Milliarden und Billionen die Rede...! Die Menge allein tut's nicht! Wie weiter vorn erläutert, sind grosse Perioden selbstverständliche Voraussetzungen, worüber man in der Fachwelt nur im Vorbeigehen spricht! (Fig.45 siehe nächstfolgende Seite)

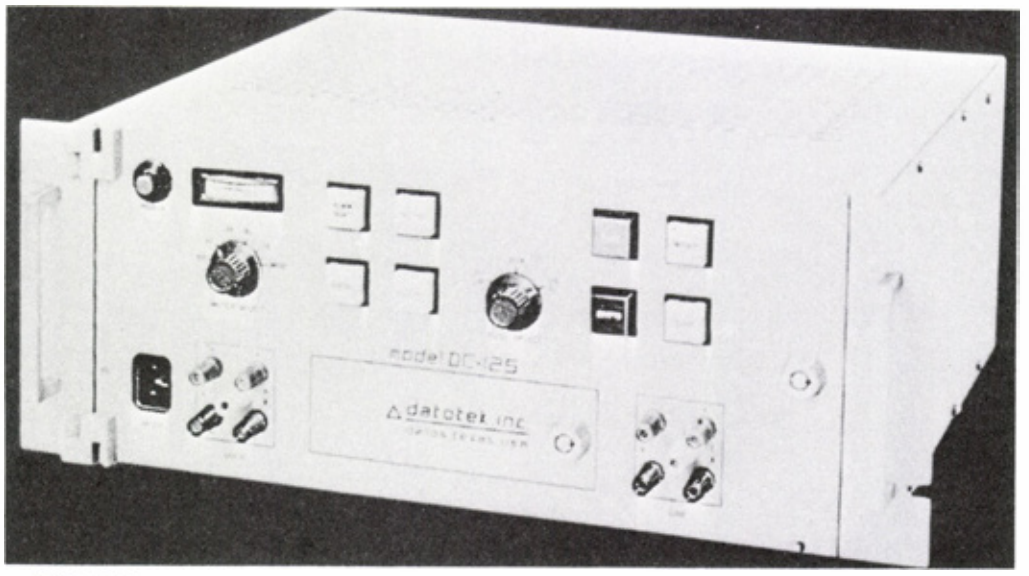


Fig. 45

Fig.46 zeigt ein kompaktes Gerät aus Schweden, wo der Schlüssel mit Lochkarte eingegeben wird. Es ist ein Fernschreibschlüsselgerät. Weiter vorn (Tab.C) wurde erwähnt, für Schlüssel in "Hardware"-form sei das idealste der Lochstreifen, besonders im Fernschreibnetzen. Lochkarten herzustellen ist schon ein bisschen mühsamer, Stanzgeräte dafür sind nicht so breit gestreut wie Fernschreiber, aber die Schweden scheinen eine Vorliebe für Lochkarten zu haben.

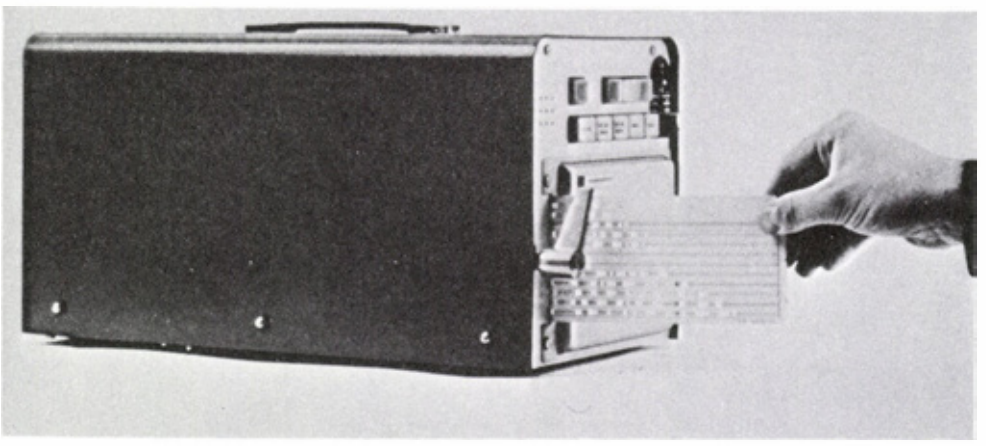


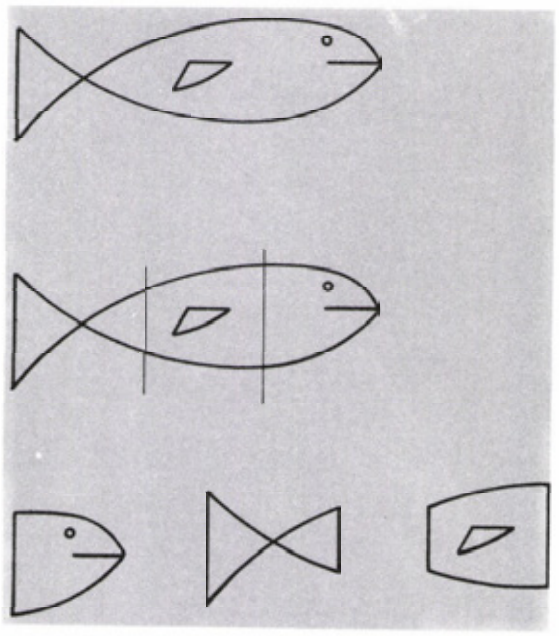
Fig. 46

7. GERAETE FUER SPRACHE

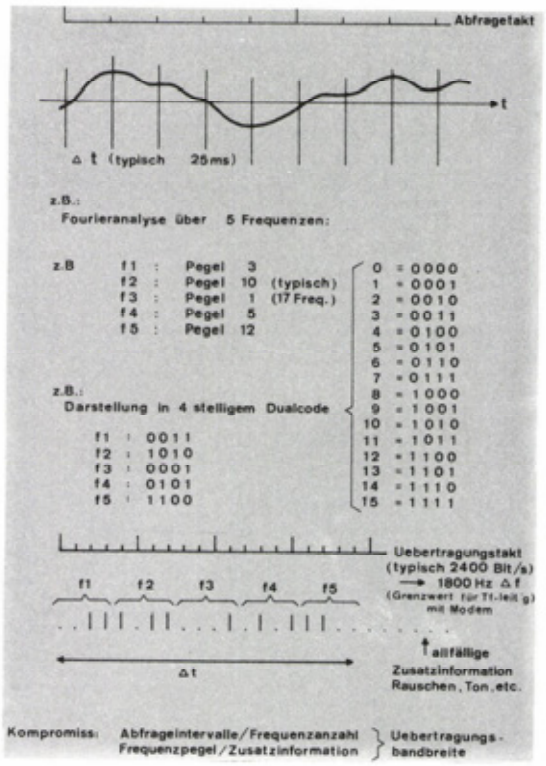
Die meisten, die sich mit diesem Problem befasst haben, glaubten vorerst, ja, die Sprache kann man doch irgendwie zerlegen und dann die Stücke permutieren.

Auf Grund eines Demonstrationsbandes mit einem Zeitachsenverschleierer ist im Vortrag nachgewiesen worden, dass dies wohl für einen einfachen primitiven Schutz genügt, vom Gesichtspunkt der heutigen Chiffriertechnik aber als unbrauchbar zu bezeichnen ist.

In den 30er Jahren und bis in den Krieg hinein, ja heute noch glauben verschiedenste Fabrikanten, mit dieser Lösung das grosse Geschäft machen zu können; die zuständigen Fachleute haben aber ziemlich rasch festgestellt, dass andere Methoden gewählt werden müssen. Das menschliche Gehirn zusammen mit dem Ohr und den millionen Jahren Entwicklung der Säugetier-Kommunikation hat akustisch zur Folge, was in Tab.D darzustellen versucht wird.



Tab. D Sprachzerhackung



Tab. E Vocoder

Der "zerhackte" Fisch in der untersten Zeile wird weiterhin als "Fisch" erkannt. Automatisch wird das Hirn sofort aus diesen Gebilden, also den Sprachfetzen, immer wieder den ganzen "Fisch" bilden, wobei die fehlenden Teile unbewusst ergänzt werden. Was wir zu hören glauben, ist dann der Text mit Repetitionen, also echomässig verhallter Klartext. So ein Demonstrationsband ist natürlich sehr bösartig, normalerweise hat man ja nicht beides, den klaren und den verschleierten Text nebeneinander, aber man kann damit zeigen, wie eben ein Zerhackgerät oder Verschleierungsgerät, Englisch "Scrambler", arbeitet.

In der Praxis dürfte es sehr nützlich sein für Polizeizwecke oder ähnliche Einsätze, wo man vermeiden will, dass der Reporter des Boulevardblattes vor dem Schutzmann am Tatort ist, aber für einen taktischen Einsatz ist so etwas schon zweifelhaft.

Man muss anders vorgehen. Wir müssen die Sprache codieren. Schon in den 30er Jahren, und später nach Veröffentlichungen von Shannon kamen Vorschläge auf zur Codierung. Es sei ganz kurz auf solche Möglichkeiten eingegangen. Die Theorien sind sehr umfangreich und die folgenden Darstellungen sind als äusserst primitive Beispiele zu werten.

Der "Vocoder", erstes Beispiel nach Tab.E ist immer noch die beste Art zur Codierung, ist aber sehr umständlich. Man macht über einen Zeitabschnitt Δt hinweg Fourier - Analysen z.B. mit 5 Frequenzen und gibt die verschiedenen Pegel, die hier willkürlich mit 3, 10, 1, 5, 12 angenommen sind, z.B. in einem 4-stelligen Dual-Code wieder.
In der untersten Zeile ist der zeitliche Ablauf dargestellt. Die Phase Δt ist hier auf die ganze Zeilenlänge erstreckt und in einem gegebenen Uebertragungstakt folgen sich die 4-stelligen Pegelinformationen der 5 Frequenzen, dazu allfällige Zusatzinformation. z.B. Rauschen "stimmhaft" oder "stimmlos" und Aehnliches.
Eine Lösung, die Kompromisse treffen muss zwischen Abfrageintervall, Frequenz-Auswahl, Anzahl der Frequenzpegel und der Zusatzinformation. Alles geht dann eben in die notwendige Uebertragungsbandbreite ein.
Anhand eines Tonbandes eines mittelguten Vocoder ist erkennbar, dass ein Vocoder nicht die Möglichkeit hat, die einzelnen Tonhöhen und die Personalität zu übertragen, man kann das für Sonderfälle wohl etwas verbessern, aber das gibt dann bücherschrankgrosse Geräte.

2-30

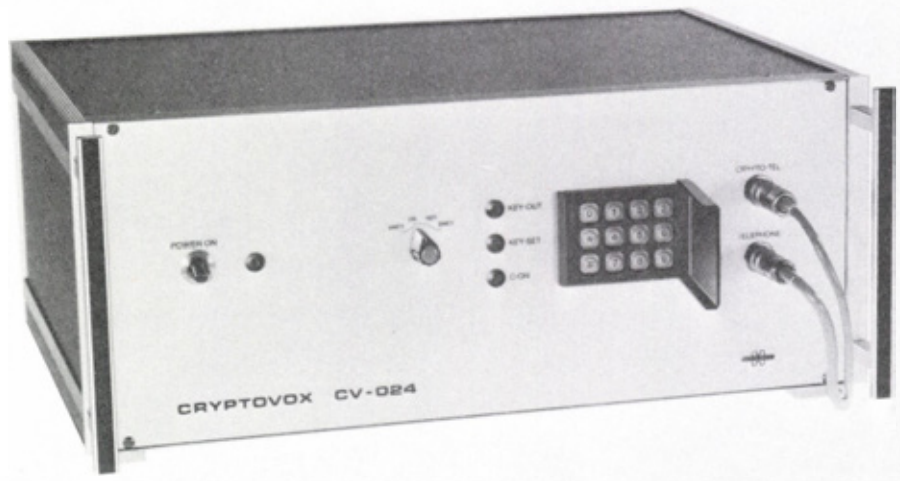
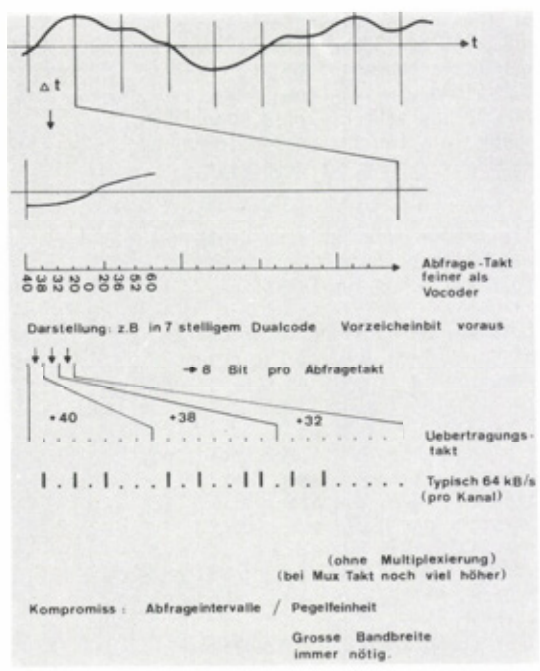
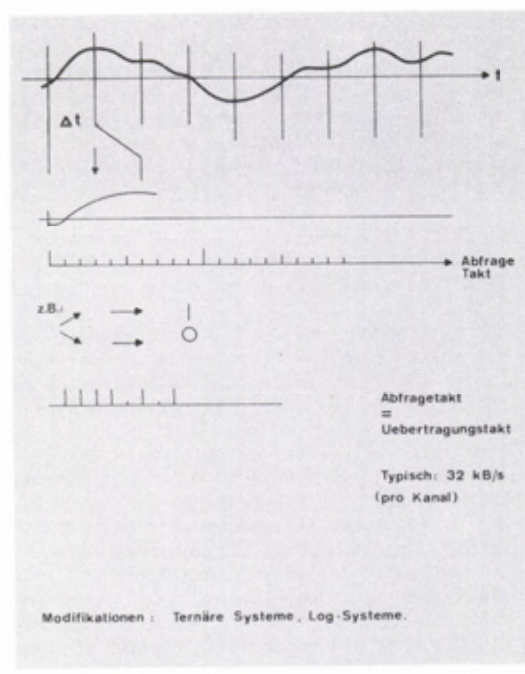


Fig. 47

Fig.47 zeigt das CV-024 der CRYPTO AG. Hier wurde ein Kompromiss getroffen; das ist ein Gerät, das über 2400 Bit arbeitet, was mittels Modem über einen guten Telephonkanal mit 1800 Hertz Mittelbandbreite übertragen werden kann. Digitaler Chiffrierteil und Modem sind in diesem Gerät enthalten.



Tab. F Pulscodemodulation (PCM)



Tab. G Δ-Modulation

Eine andere Möglichkeit ist die Pulscodemodulation (PCM, Tab.F). Sie wird hauptsächlich bei Postübertragungen angewendet, ebenso bei Satellitenübertragungen. Die zu codierende Information wird wieder in Zeitabschnitte Δt aufgeteilt. In Zeile 2 ist ein Δt vergrössert dargestellt. Der Absolutpegel, dargestellt in Dualcode wird übertragen, hier z.B die Werte 40, 38, 32 usw. Die Uebertragungsgeschwindigkeit beträgt dabei z.B. 64 kbit/s. Man sieht, dass diese codierte Information nicht mehr über eine Telephonleitung übertragen werden kann. PCM ist daher für Telephon-Sprachverschlüsselung nicht geeignet.

Die sauberste Lösung bildet die Δ-Modulation (Tab.G), die in den 60er Jahren entwickelt wurde. Sie arbeitet mit der gleichen Uebertragungsfrequenz wie die Abtastfrequenz. Dabei wird ein Zeitabschnitt Δt betrachtet. Geht der Kurvenverlauf am Ende von Δt nach oben, wird eine 1 übertragen, geht er nach unten, so ist es eine 0. Auf diese Weise können vernünftige Lösungen realisiert werden.

Fig. 48

Fig.48 zeigt das CRYPTOVOX, das sich seit einigen Jahren bestens bewährt hat. Es ist kombiniert mit einem UKW-FM-Funkgerät. Das Gerät ist für Mikrotelephonbetrieb gedacht und für maximale Persönlichkeitserkennung von Mikrophonkapsel zu Hörer entwickelt. Mit einem gewöhnlichen FM-Empfänger kann auf der gleichen Frequenz wie das CRYPTOVOX nur Rauschen empfangen werden, d.h. eigentlich digitale Impulsfolgen; eine Anpeilung wird daher stark erschwert. Man suche einmal einen unbekannten Rauschsender auf unbekannter Frequenz mit einem Peilempfänger!

Für einen Betrieb über Telephonleitungen oder Kurzwellenstrecken eignet sich dieses Verfahren aber nicht. Man muss eine Mischung zwischen digitaler Verarbeitung und "Zerhackung" wählen, da der Uebertragungskanal nur analoge (sprachähnliche) Information überträgt. Eine Möglichkeit besteht darin, die Zerhackung auf 2 Ebenen oder auf 2 Achsen durchzuführen. Es seien hier einige Geräte gezeigt (Fig.49, 50, 51, 52), ohne auf deren Klassifizierung näher einzugehen.

Fig. 49

Fig. 50

Fig. 51

Fig. 52

Fig.53 zeigt ein Gerät mit zweiachsigem abwechselnden Code. Man zerhackt in der Zeitachse und in der Frequenzachse, dazu gehört ein Telephonkoppler. Der Telephonkoppler ist ein zweischneidiges Schwert, es geht noch bei Geräten dieser Art, wo eben die Information aus relativ groben Sprachfetzen besteht. Sobald es komplizierter wird, funktioniert das nicht mehr. Die gewöhnlichen Kohlemikrophone, die immer noch weltweit im Einsatz sind, geben sehr rasch den Geist auf, wenn sie längere Zeit ruhig in Horizontallage liegen bleiben; im direkten menschlichen Gespräch werden sie dauernd geschüttelt und sind senkrecht gelagert!

Fig. 53

2-33

Fig. 54

Fig. 55

Fig.54 zeigt das"CRYPTOPHON 1100" zusammen mit einem fremden Funksprechgerät (man sieht, dass auch Weltfirmen oft so zusammenarbeiten können, dass die Zusammenarbeit nur durch die Geräte besorgt wird!). Fig.55 zeigt das Brudergerät in Militärverpackung.

Fig. 56

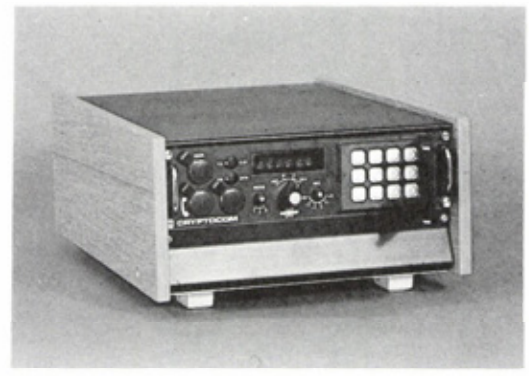


Fig. 57

Fig.56 zeigt ein Gerät aus Deutschland mit einem schönen Telephon darauf. Es wird als "Digital Scrambler" angeboten. Man muss hier aber aufpassen. Es gibt viele Leute, die von "Digital Scrambler" reden. Der düpierte Kunde glaubt dann: "aha, da ist eine digitale Verschlüsselung drin", und zum Schluss stellt sich heraus, dass das einzige, was digital ist, die Einstellelemente oder eben den Takt im Gerät drin betreffen!

Fig.57 zeigt eine Möglichkeit, wie die CRYPTO AG das Problem zu lösen versucht hat. Anhand einer Tonbandvorführung ist feststellbar, dass bei diesem zweiachsig arbeitenden, übers Kreuz permutierenden Gerät eine Texterkennung nicht mehr möglich ist.

Fig 58

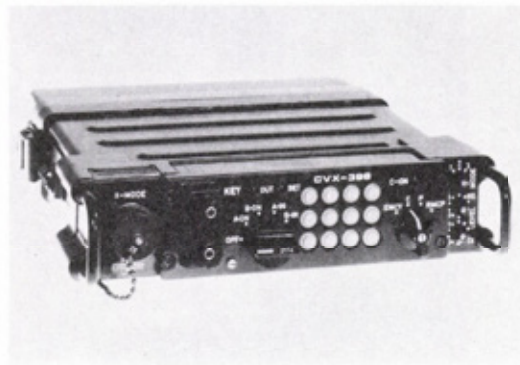


Fig. 59

Fig.58 zeigt die feldtaugliche Version. Es wird hier effektiv digital gearbeitet. Der Text wird zweimal umgeformt. Man hat vorerst eine Δ-Modulation. Der ganze digitalisierte Textstrom wird blockweise eingespeichert und dann in zwei Frequenzachsen unabhängig in 40ms langen Digitalpaketen übers Kreuz permutiert, was ungefähr 4.10^{11} Permutationsmöglichkeiten ergibt. Das Ganze wird wieder in einen Tonfrequenzzug umgeformt und auf die Leitung gegeben. Der Schlüsselgenerator kann auf 10^{32} Grundeinstellungen gebracht werden. Natürlich kommt es vor, dass ein Paket am Anfang der Speicherperiode wieder zum Vorschein kommt, das am Ende oder in der Mitte des gleichen Frequenzbandes lag, dann kommt unter Umständen doch noch eine "Fischgeräte" durch, um beim anfänglich gewählten Anschauungsbild (Tab.D) zu bleiben. Aber zur vernünftigen Analyse ist hier nichts zu holen.

Die wohl jüngste Technik, wie sie hier vorliegt, verlangt nach hochintegrierten Schaltungen. Das CRYPTOCOM ist in CMOS aufgebaut. Bei den Digitalgeräten, (die CRYPTOVOX sind jetz ungefähr 6 Jahre alt), ist man auch einen Schritt weiter gekommen: Fig.59 zeigt das Gerät CVX-396, welches genau zum weltweit verbreiteten Sprechfunkgerät PRC-77 passt, das den meisten Uebermittlern bekannt sein dürfte. Alles hermetisch verschlossen. Der Vorderteil kann als Fernsteuerungseinheit abgenommen werden und das Ganze verbraucht nur noch ein Watt an Leistung! Also das Chiffrieren ist heute nicht mehr so ein kompliziertes Ding.
Man kann das CVX-396 mit dem PRC-77 zusammenschnallen und es bietet die Möglichkeit, zwei Grundschlüssel einzuspeichern. Dazu dient die Tastatur, die weiter vorn erwähnt ist.

Fig.60 zeigt einen Zerhacker, der an ein Handy-Talky angeschnallt wurde. Dass man bei den "Handy-Talky" aber nicht schläft, zeigt Fig.61: Das Gerät wurde in Wiesbaden anfangs Oktober erstmals vorgestellt. Das sind "Handy-Talky" mit Delta-Modulation und Verschlüsselung, alles miteingebaut!
Allerdings sieht man keine Schlüsseleinstellelemente, die Dinger werden fix programmiert und dann verteilt. Für Polizeieinsatz sehr geeignet. (Wie der kürzlich knapp vermiedene Ueberfall auf das Frachtlager der Swissair in New York zeigte, arbeiten die Ganoven heute auch mit moderner Elektronik, die Polizei muss somit nachziehen!) Für taktischen Einsatz klappt das aber unmöglich, man kann ja die Geräte nicht jeden Tag einsammeln und dann wieder neu programmiert an die Front verteilen!
Das CVX-396 (Fig.59) ist heute für militärischen Einsatz als optimale Lösung anzusehen. Es ist etwas grösser als ein "Handy-Talky", dafür auch etwas robuster, aber das Bild 61 soll zu erkennen geben, wie rasch die Technik vorwärts geht.
(Fig.60 + 61 siehe nachfolgende Seite)

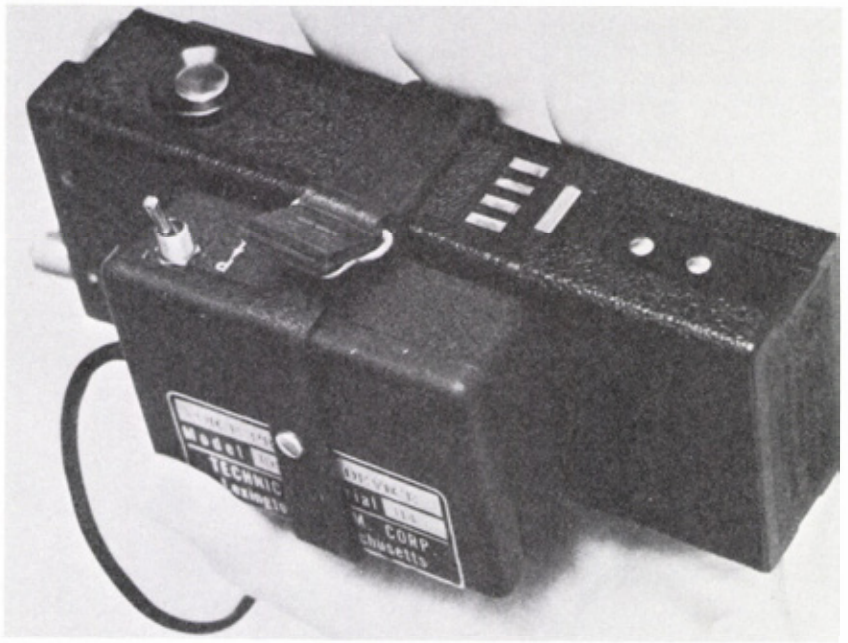


Fig. 60

Fig. 61

8. GERAETE FUER SCHNELLE DIGITALFOLGEN

Es gibt Bedarfsfälle für multiplexierte Systeme, z.B. Richtstrahlanlagen, oder bei Rechenanlagen, einerseits vom Rechner an eine Aussenstelle und anderseits vom Rechner zum eigenen Speicher, besonders wenn Information aus Sicherheitsgründen für längere Zeit ausser Haus gelagert wird. Die Lösung für Multiplexsysteme ist grundsätzlich unproblematisch; man kann ein Gerät nehmen, das eben den Datenstrom umsetzt und den einkommenden wieder zurückversetzt.

Fig.62 zeigt ein Breitbandgerät für Mikrowellenstrecken; oben das eigentliche Schlüsselgerät CRYPTOPLEX, darunter 2 Multiplexer, die je 8 Telephonkanäle verarbeiten können. Das Gerät arbeitet bis zu 2 Mbit/sec vollautomatisch im Duplexbetrieb. Die Schlüsseleingabe erfolgt mittels Lochstreifenabtaster, der wasserdicht abgeschlossen werden kann.

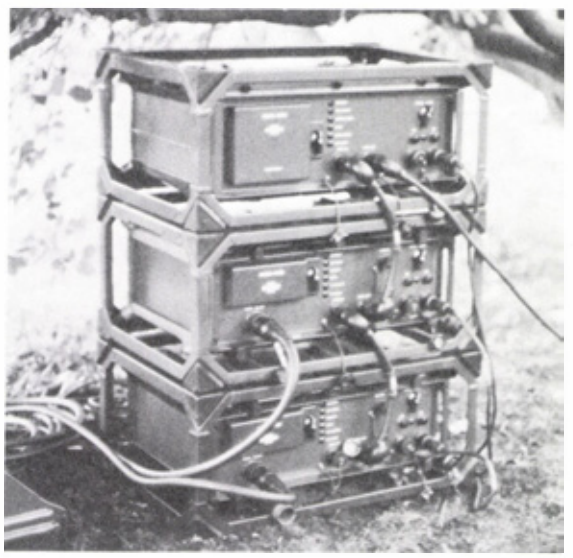


Fig. 62

Verschlüsselt wird logischerweise mit textabhängiger Beeinflussung, da ja digital gearbeitet wird. Die Aenderung des Grundschlüssels ist also aus kryptologischen Gründen nicht mehr unbedingt notwendig, und nur taktische Ueberlegungen verlangen noch, dass der Schlüssel grundsätzlich alle Monate oder alle 14 Tage geändert werden soll. Fig.63 zeigt einen Entwurf, der ähnliche Lösungen in dieser Richtung anstrebt.

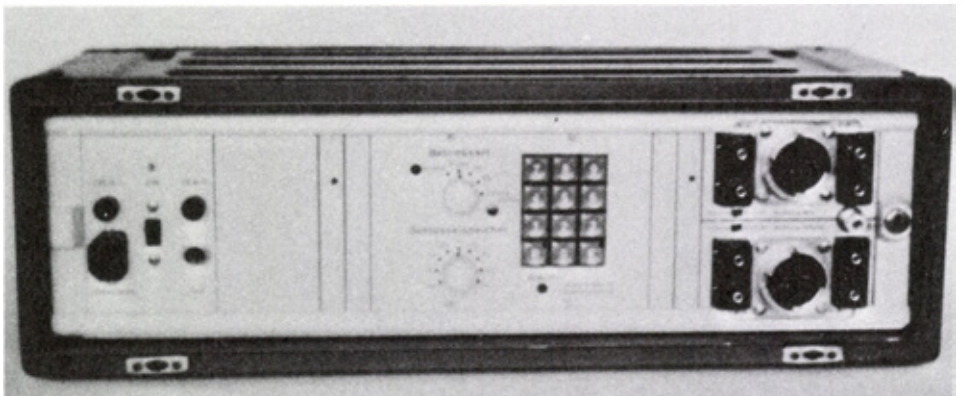


Fig. 63

Die ganze Welt schreit heute nach Datenschutzgeräten. Bei Grossrechenanlagen ist das Problem aber kompliziert. Es gibt wohl sogenannte "Datenschutzgeräte", wie z.B. in Fig.64 dargestellt, ein Gerät, das an der Hannover-Messe Bewegung verursacht hatte und in den Tageszeitungen teilweise als weltbewegende Neuheit vorgestellt wurde. Der Schlüssel wird mit einer Lochkarte eingegeben; diese stellt aber bereits einen Kompromiss dar, denn es ist nicht eine normale sogenannte IBM-Lochkarte, sondern eine spezielle kleine Karte. Das gezeigte Beispiel ist unter Umständen noch unproblematisch, es wird aber schwierig, wenn man näher in die Details geht.

Viele Rechner sind mit den Aussenstellen dauernd im Dialog. Dies ist die Achilles-Verse! Der Dialog findet in einer Sprache statt, die an und für sich ganz bestimmten Gesetzen folgen muss, und die man deshalb nicht verschlüsseln darf, da sonst das Gerät Fehleralarm gibt. Man muss dauernd umschalten, und wenn dann "heisse" Information gesendet werden soll, und verschlüsselt werden muss, muss man in Crypto-Lage. Dann kommt eine Rückfrage vom Gerät: "Ist diese Gruppe in Ordnung?" Das muss wieder in Klartext gehen, dann muss verschlüsselt werden, wieder entschlüsselt usw. Diese Probleme können nur gelöst werden, falls der Kunde den ganzen Verfahrensablauf seiner Anlage kennt. In 99% aller Fälle kann er das nicht. Der Computerlieferant ist äusserst zurückhaltend, wenn Aussenstehende ihn um Verfahrensprozeduren angehen, und so muss der Chiffriergerätefabrikant in mühsamer Kleinarbeit Forschung betreiben, die mit der Chiffrierung an und für sich nichts zu tun hat. Es gibt bis heute also kein Datengerät, das man verkaufen kann wie ein Fernschreibschlüsselgerät, jedes bestehende Datengerät ist für einen bestimmten Computer massgeschneidert

Fig. 64

Fig.65 zeigt das "CRYPFAX" aus England, das auch für Faximileübertragung dient. Beim Gerät in Fig.66, das im kommerziellen Sektor eingesetzt wird, sind die Probleme der Klar-Geheim-Umschaltung nicht so kompliziert. Fig.67 schliesslich zeigt eine Lösung, die am besten umschrieben wird als "eierlegende, wassergehende Vollmilchsau", oder: "geländegängiger Amphibienflug-Rolls-Royce". Dieses Gerät wurde als Studienobjekt für einen militärischen Kunden entwickelt, der Datenschlüsselgeräte haben wollte, die in allen ihm bekannten Fällen einsetzbar sind. Die Gehäusekonstruktion ist wie bei der CRYPTOPLEX-Gruppe (Fig.62), und die Uebertragungsgeschwindigkeit beträgt 50...9600Baud. Das Gerät besitzt alle Möglichkeiten, die heute vorkommen: Synchronbetrieb, Start-Stop-Betrieb, Duplexbetrieb, Abrufbetrieb, Impulsbetrieb, Wortbetrieb, Blockbetrieb usw.Man erkennt, dass das Problem "Datenverschlüsselung"enorm komplex werden kann, wenn es universell gelöst werden soll. Dass die CRYPTO es lösen kann, beweist das Beispiel Fig.67. Ein serienmässiger Verkauf kommt kaum in Frage, aber Masskonfektion kann daraus getrieben werden.

Fig. 65

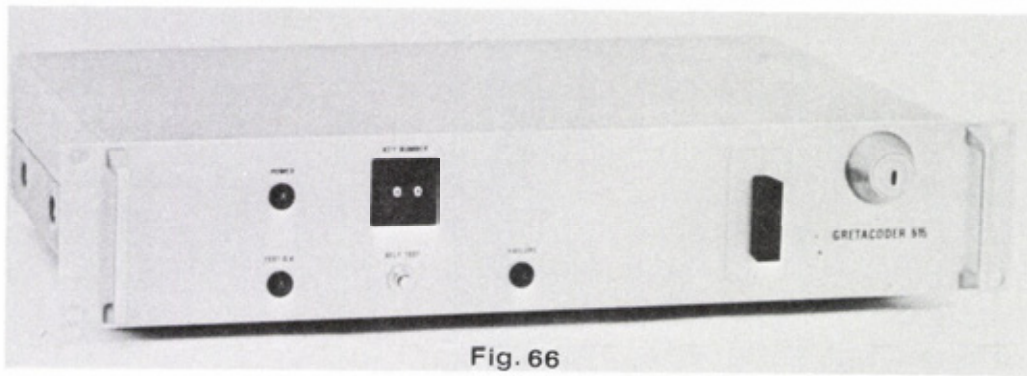


Fig. 66

Fig. 67

F I G U R E N V E R Z E I C H N I S

Fig. 1	"Skytale", Sparta, Athen
Fig. 2	"Cäsar", Rom
Fig. 3	Röckstein, Wikinger, ca.9.Jh.
Fig. 4	Titelblatt zu "Steganographie" 1621
Fig. 5	Dechiffriergerät L.B.Alberti, 1430 (Rekonstruktion)
Fig. 6	Hilfszylinder nach E.Bazéries, 1891 (Jefferson ca.1795)
Fig. 7	Erste bekannte Chi-Maschine (Rekonstruktion) Rittmeister Gripenstierna, 1786
Fig. 8,9,10	Rechnung an den Hof Gustav Adolfs III
Fig. 11	Betrieb der Maschine
Fig. 12	Chi-Maschine von Wheatstone, 1867
Fig. 13	Chi-Gerät A-22 von A.G. Damm, 1918
Fig. 14	Elektromech.Chi-Komplex von A.G. Damm, ca. 1922
Fig. 15	Urmodell B-21, Elektromech.Chi-Gerät, B.C.W.Hagelin, 1925
Fig. 16	Französisches Lizenzgerät B-211, Ericsson France, 30er Jahre
Fig. 17	Grundprinzip der B-21
Fig. 18	Original "Enigma", Berlin 20er/30er Jahre
Fig. 19	C-35, B.C.W.Hagelin, vollmechanische Chi-Maschine mit Druckwerk
Fig. 20	USA-Lizenzgerät M-209, 1942...44 (140'000 Stk.gebaut)
Fig. 21	Tastaturvariante BC-543, A.B.Cryptotechnik Stockholm, 40er Jahre
Fig. 22	Deutsche Kopie C-41, 1944, Wanderwerke Chemnitz
Fig. 23	BC-621 Kombination bestehend aus Chi-Maschine C-52 und Klaviatur B-621. Dazu Lochstreifengerät PEB-61, CRYPTO AG
Fig. 24	HX-63, off-line Chi-Maschine mit Volltastatur und Doppeldruckwerk; unregelmässig vorgeschobene 41er Durchgangsräder, CRYPTO AG
Fig. 25	CD-57, nicht schreibende vollmech.Chi-Maschine, CRYPTO AG
Fig. 26	Rückgekoppeltes Schieberegister
Fig. 27	Rückgekoppeltes Schieberegister, Variante zu Fig.26
Fig. 28	Simulation eines 26er Systems mit Digitalinformation
Fig. 29	Umcodierung dualer Information zu Permutationszwecken
Fig. 30	Homonyme Zifferncodierung
Fig. 31	Exclusive-Oder Verknüpfung
Fig. 32	H-4605, off-line Chi-Maschine mit elektronischer Logik, CRYPTO AG
Fig. 33	Lochstreifengerät PEH-72 zu H-4605, CRYPTO AG
Fig. 34	TSTL-2000, off-line Chi-Maschine mit Primärtextanzeige, elektronische Logik, MILS Elektronik
Fig. 35	9 EC 420, off-line Chi-Maschine mit integrierten Lochstreifenzusätzen, Volltastatur flieg.Doppeldruckwerk, elektronische Logik, Philips Schweden
Fig. 36	HC-570 CRYPTOMATIC elektronische off-line Chi-Maschine, Thermodrucker, Primäranzeige, Integrierte Lochstreifenzusätze, Volltastatur, dazu Telephonkoppler, CRYPTO AG
Fig. 37	HC-520 CRYPTOMATIC tragbares Handgerät, zu HC-570 kompatibel, Volltastatur, Flüssigkeitskristallanzeige, 800-Zeichenspeicher, CRYPTO AG
Fig. 38	MA 4210 tragbares Handgerät mit Ziffernbigrammen als Chi-text information, RACAL
Fig. 39	905 GRETACODER, tragbares Handgerät mit Wanderlichtpunkt, GRETAG
Fig. 40	Prototyp zu on-line FS-Chi-Gerät für CCITT, Code No.2 & ETK-Code ($^{14}_{5}$) Stockholm 1947
Fig. 41	TA-1, Elektromech.on-line FS Chi-Gerät, TRANSVERTEX
Fig. 42	T-450, CRYPTROL, vollelektron. on-line Chi-Gerät, Feldversion, CRYPTO AG
Fig. 43	T-450, Büroversion, CRYPTO AG

Fig. 44	TC-812, Vollelektron. On-line Chi-Gerät, GRETAG
Fig. 45	DC-125, Vollelektron. On-line Chi-Gerät, DATOTEK
Fig. 46	TC-13, Vollelektron. On-line Chi-Gerät, TRANSVERTEX
Fig. 47	CV-024, Vocoder-Sprach Chi-Gerät mit Modem, CRYPTO AG
Fig. 48	CSE-280, CRYPTOVOX Digitales Sprachschlüsselgerät mit 500-Kanal UKW Funksprechgerät, CRYPTO AG
Fig. 49	SR-22, Digitales Sprachschlüsselgerät, TRANSVERTEX
Fig. 50	105-RV, Fix-Code Verschleierer mit Frequenzpermutation, TCC
Fig. 51	CRYPTEX, digit. Sprachschlüsselgerät darunter MARVOX Vocoder, MARCONI
Fig. 52	"202", 2-Band Sprachschleiergerät, APPL.DATA CORP.
Fig. 53	307-VPD, Sprachschleiergerät mit Telephonkoppler, TCC
Fig. 54	CRYPTOPHON 1100, Sprachschleiergerät (mit Telefunken Funksprechgerät), BROWN-BOVERI
Fig. 55	VERICRYPT 1600, Feldtüchtiges Sprachschleiergerät, BROWN-BOVERI
Fig. 56	dtg 9200, Büro-Sprachschleiergerät,KUKLA
Fig. 57	CRM-008, CRYPTOCOM, Analog-Sprachschlüsselgerät mit digitaler Signalverarbeitung, CRYPTO AG
Fig. 58	CRM-008, Feldversion, CRYPTO AG
Fig. 59	CVX-396, CRYPTOVOX, Digitales Sprachschlüsselgerät für extreme Feldbedingungen, CRYPTO AG
Fig. 60	105 RP, Fix-Code Sprachschleiergerät am "Handy-Talky" angeschnallt, TCC
Fig. 61	MX-300, Digital arbeitendes Schlüssel-Funksprechgerät, fix codierbar, MTOROLA
Fig. 62	CRYPTOPLEX Gruppe, Oben: MCC-314 Breitband Duplex-Schlüsselgerät, Unten: zwei 8-Kanal Multiplexer AMD.310, CRYPTO AG
Fig. 63	VERICRYPT 2000, Breitband-Duplex-Schlüsselgerät, BROWN-BOVERI
Fig. 64	TELEKRYPT 8, Datenschutzgerät, AEG-TELEFUNKEN
Fig. 65	CRYPFAX, Digital arbeitendes Chi-Gerät für Bildtelegraphie, MARCONI
Fig. 66	515 GRETACODER, Datenschutzgerät, GRETAG
Fig. 67	CRYPTRONIC, CRT-320, Feldtaugliches, universell einsetzbares Daten-Chi-Gerät für verschiedenste Betriebsarten, 50...9600 Baud, CRYPTO AG