BAYERISCHE AKADEMIE DER WISSENSCHAFTEN
MATHEMATISCH-NATURWISSENSCHAFTLICHE KLASSE

ABHANDLUNGEN · NEUE FOLGE, HEFT 176

Friedrich L. Bauer

Die Komödie der Irrungen im Wettstreit der Kryptologen

Vorgetragen in der Sitzung
vom 14. Dezember 2007

MÜNCHEN 2008

VERLAG DER BAYERISCHEN AKADEMIE DER WISSENSCHAFTEN

IN KOMMISSION BEIM VERLAG C. H. BECK MÜNCHEN

ISSN 0005–6995
(Abhandlungen – Bayerische Akademie der Wissenschaften,
Mathematisch-Naturwissenschaftliche Klasse)

ISBN 978 3 7696 0972 1

Gesamtherstellung: Druckerei C. H. Beck, Nördlingen
Gedruckt auf säurefreiem, alterungsbeständigem Papier
(hergestellt aus chlorfrei gebleichtem Zellstoff)
Printed in Germany

Inhalt

A COMEDY OF ERRORS

Unter Anspielung auf Shakespeares Schauspiel *Die Komödie der Irrungen* schrieb Gordon Welchman (1906–1985), neben Alan Turing (1912–1954) der bedeutendste britische Mathematiker im Dechiffrierzentrum Bletchley Park und einer der Väter des Erfolgs der Briten im Zweiten Weltkrieg:[1] "*That we managed to stay in the game until the end of the war was made possible only by a comedy of errors committed by the Germans*". Welchmans Beitrag zu diesem Erfolg war gegen die Rotor-Chiffriermaschine ENIGMA der Wehrmacht gerichtet, aber mit gleichem Recht hätte sein etwas älterer Kollege Max Newman (1897–1984) diesen Ausspruch wagen können im Hinblick auf die deutschen Chiffrierfernschreiber, insbesondere das Gerät SZ 40/42 von Lorenz. Die deutsche militärische Seite war über das Ende des Krieges hinaus ahnungslos.

Umgekehrt war es Wilhelm Tranow vom B-Dienst der Kriegsmarine gelungen, 1939 und 1940 die Naval Cipher No. 1 der Royal Navy zu lesen, und Hans Rohrbach (1903–1993), in der Gruppe Pers Z im Auswärtigen Amt des Reiches tätig, wäre auch zu einer Replik in der Lage gewesen: er war der Motor einer großangelegten Operation, die 1942–1944 in ein für absolut sicher gehaltenes Chiffrierverfahren der US-Diplomatie eindrang: ein polyalphabetisches Streifenverfahren, genannt O-2 (ähnlich dem weithin verbreiteten, vom US-Militär benutzten M-138) mit mehreren Dutzend unabhängigen Alphabeten.

Der pikante Hintergrund des Ausspruchs ist, daß in Kriegs- und auch in Friedenszeiten die jeweiligen Chiffrierdienste sich bemühten, den potentiellen Gegner zu täuschen, in Sorglosigkeit zu wiegen, ihre Fähigkeiten geschickt zu verbergen. So nahmen die Briten im Seekrieg den Verlust von Material und Menschen hin, um keine verräterischen Hinweise über den Umfang ihres Eindringens in die deutschen Chiffriersysteme zu geben. Mit List und Tücke, vor allem aber mit verbissener Nachhaltigkeit versucht man, einmal erzielte kleinere Einbrüche auszunutzen zum Ausbau des Wissensstands über die gegnerischen Umstände, Absichten, Wortwahlen, Gewohnheiten, Fehleinschätzungen, Nachlässigkeiten, Dummheiten, Führungsschwächen. Und der schlimmste Feind sitzt im eigenen Boot: Ahnungslosigkeit, Überheblichkeit, 'das Unbequeme nicht wahr haben wollen'.

Das zeichnete vor allem die deutsche Seite aus. Es galt aber auch für die Briten, wie der Kryptologiehistoriker Ralph Erskine am 6. Oktober 2006 in der *Times* berichtete:

TUNNY[2]*, which was used mainly between the German High Command and army groups, provided more strategic intelligence than ENIGMA. TUNNY decrypts between June and October 1942 revealed that Kriegsmarine B-Dienst codebreakers were solving the principal Allied convoy code. In a massive blunder, that code was not replaced until June 1943, resulting in huge losses of ships and human life, especially during the deadly convoy battles of march 1943. The delay was largely organizational, but senior managers at Bletchley cannot have pressed hard enough to get it changed.*

[1] Gordon Welchman, *The Hut 6 Story*. M&M Baldwin, Cleobury Mortimer 1997, p. 163.
[2] Schlüsselzusatz SZ 40, SZ 42.

Soweit das Verhältnis der Deutschen zu ihren Gegnern, den Briten und Amerikanern. Parallel dazu ist das Verhältnis der Amerikaner zu ihrem Gegner Japan zu betrachten. Die Kryptologen der Vereinigten Staaten müßten sich da wiederum nicht lumpen lassen: William F. Friedman, ihr großer alter Mann, hätte sich brüsten können, Fehler der japanischen Chiffrierer ausgenutzt zu haben, um mit seiner Gruppe, in der sich Genevieve Grotjan und Leo Rosen besonders hervortaten, die im Februar 1939 eingeführte japanische Rotor-Chiffriermaschine "Typ B" (US Deckname PURPLE) bereits im September 1940 zu bezwingen. Dies wiederum hätte den schon früher für Pers Z im Auswärtigen Amt arbeitenden Werner Kunze veranlassen können, seinerseits auf sein schon 1936 gelungenes Eindringen in die japanische Katakana-Maschine (US Deckname ORANGE), die einen schweren Entwurfs-Fehler aufwies, hinzuweisen. Die Deutschen, im Krieg Japans Verbündete, hatten natürlich den japanischen Botschafter nicht gewarnt. Im Wettstreit der Kryptologen ist Mißtrauen selbst dem Freund gegenüber die Regel — Großbritannien und die Vereinigten Staaten taten sich bis zum BRUSA Pakt im Mai 1943 schwer, in der Kryptanalyse zusammenzuarbeiten, Reibungen und Spannungen konnten auch später nicht völlig ausgerottet werden.

Und so könnte man fortfahren, wobei ein Seitenblick auf den Franzosen Étienne Bazeries (1846–1931) abfällt, der ein erfolgreicher Codebrecher war und gegen Ende des 19. Jahrhunderts sich dann hinreißen ließ, selbst ein „unbrechbares" Verfahren anzupreisen (*Je suis indéchiffrable* benutzte er als Beispielsatz); er mußte die Blamage hinnehmen, daß sein Konkurrent Gaëtan de Viaris seine Chiffrierung brach. Der vor, während und nach dem Ersten Weltkrieg immer noch sehr erfolgreiche französische Dienst mußte andererseits einstecken, daß in den dreißiger Jahren, wie Erich Hüttenhain[3] berichtete, seine Kryptanalysten 1938 in das sog. fld-Netz der französischen Wehrkreise eindrangen. Deshalb hatte die Wehrmacht, als sie 1940 Frankreich angriff, trotz Hitlers strategischen und taktischen Fehlern leichtes Spiel.

Man könnte auch in der Geschichte zurückgehen bis ins ausgehende Mittelalter am päpstlichen Hof, weiter noch bis zu den Muslims in Bagdad — Al-Qalqashandi, Al-Khalīl, Al-Kịndī, ja sogar bis zu Julius Caesar — dessen System, jeden Buchstaben durch den im Alphabet drittnächsten Buchstaben zu ersetzen, so schrecklich einfach war, daß es sicher keinem Angriff lange standhielt. Leider weiß man nicht, wer es zum ersten Mal brach.

Man weiß aber auch nicht, wem das zuletzt gelang — jedenfalls berichtete Frank Rowlett (1908–1998), aus Friedmans Mannschaft, daß Friedman sehr erstaunt war, als er ihm um 1935 zeigen konnte, daß die Japaner im diplomatischen Verkehr gelegentlich ein monoalphabetisches System verwendeten.

Die Geschichte der Kryptologie lehrt, daß der sog. 'unbefugte Entzifferer' von den Fehlern des Gegners lebt.

Charakterisierung der Irrungen

Genug des grausamen Spiels des sich gegenseitig aufs Kreuz legen. Auf welchen Fehlern beruht es? Gordon Welchman faßt es in seiner Publikation folgendermaßen verkürzt zusammen: die Fehler, von denen er spricht, können bereits von den Entwerfern der Kryptosysteme gemacht werden — Systembedingte Fehler; unabhängig davon aber auch — womit man stets rechnen muß — bei ihrem undisziplinierten Gebrauch.

Hier ist die Schuld jedoch nicht immer beim einfachen Chiffriersoldaten oder Codeschreiber zu suchen, dem übrigens von ignoranten Vorgesetzten gern unmögliches abverlangt wird — die Schuld liegt nicht selten auch bei hohen und höchsten Vorgesetzten, die uneinsichtig, wenn nicht gar arrogant sind. Für einschlägige Beispiele haben Generäle und Botschafter reichlich gesorgt, von den bekannteren sei der amerikanische Sonderbotschafter Robert Murphy (1894–1978) und der deutsche Konteradmiral Eberhard Maertens genannt. Und überhaupt neigt man in diesen Kreisen eben gern dazu, den Gegner für dumm zu halten, wofür Kapitän zur See Heinz Bonatz[4], ehemals Leiter der deutschen Marinefunkaufklärung während des 2. Weltkriegs, ein leuchtendes Beispiel abgibt, der noch 1970 ernsthaft die Frage aufwarf, ob die Polen, wie Władysław Kozaczuk 1967 berichtet hatte, tatsächlich das Rätsel der ENIGMA gelöst hätten — von den Briten konnte er zu diesem Zeitpunkt noch nichts wissen. Die britischen Hintergründe deckte erst 1973 der französische General Gustave Bertrand auf. Die erste authorisierte britische Veröffentlichung wurde 1974 Captain Frederick W. Winterbotham gestattet, der Verbindungsoffizier zu Winston Churchill war.

[3] Erich Hüttenhain, *Einzeldarstellungen aus dem Gebiet der Kryptologie*, Typeskript in der Handschriftenabteilung der Bayerischen Staatsbibliothek, Cgm 9304a .

[4] Heinz Bonatz, *Die deutsche Marine-Funkaufklärung 1914–1945*. Darmstadt, Wehr und Wissen 1970.

SYSTEMBEDINGTE EINBRUCHSMÖGLICHKEITEN

Die Geschichte der Kryptologie zeigt also insbesondere ein Wechselspiel auf zwischen dem Kryptographen, der sich im Glauben an die praktische Unbrechbarkeit eines Kryptosystems wiegt, und dem Kryptanalysten, der zäh und listig den Einbruch versucht, — ein Spiel, bei dem sich oft die Waage mal nach der einen, mal nach der anderen Seite neigt.

Zum Glauben an die praktische Unbrechbarkeit eines Kryptosystems neigen insbesondere die Schöpfer eines solchen, eines Chiffriergeräts oder einer Chiffriermaschine. Hier mögen kaufmännische Gründe eine Rolle spielen, wie sie etwa bei Alexander von Kryha (∗1891) vorlagen, dem geschäftstüchtigen Erfinder der nach ihm benannten Chiffriermaschine, die sich zwar in einem glänzenden Nickelgehäuse befand, aber durch die zu geringe Periode 442 der polyalphabetischen Chiffrierung nur wenig Sicherheit bot — der große amerikanische Kryptologe William F. Friedman (1891–1969) brach ein Kryha-Chiffrat in der Mittagspause.

Solche Gründe lagen sicher nicht vor bei dem schon erwähnten Étienne Bazeries, einem sehr fähigen und erfahrenen französischen Kryptologen, Offizier und ab 1899 am Quai d'Orsay tätig, der selbst, indem er ihre Schwächen aufzeigte, zahlreiche dem französischen Generalstab vorgelegte Erfindungen von Chiffriersystemen zuschanden gemacht hatte — darunter eine von dem Marquis Gaëtan Henri Léon de Viaris (1847–1901). Bazeries erfand 1891 den Chiffrierzylinder, den schon gegen Ende des 18. Jahrhunderts Thomas Jefferson (1743–1826) angegebenhatte, wieder. Der Marquis de Viaris rächte sich dadurch, daß er seinerseits sogar eine allgemeine Methode angab, um den von Bazeries erfundenen Chiffrierzylinder zu brechen.

Bazeries hatte nämlich eine winzige Kleinigkeit übersehen: Die durch Merkverse erzeugte polyalphabetische Chiffriertafel enthielt zwar in jeder Zeile jedes Alphabetzeichen genau einmal, aber in den Spalten kamen einige Zeichen mehrfach vor, wofür andere fehlten. Über die fehlenden Zeichen gelingt in der Methode von de Viaris der Einbruch. Als der amerikanische Kryptologe Oberst Parker Hitt (1877–1971) 1914 ein dem Chiffrierzylinder entsprechendes Streifengerät in die U.S.Army einführen wollte, wurde er unter Hinweis auf de Viaris abgewehrt; 1922 stellte jedoch der Major, der spätere Generalmajor Joseph O. Mauborgne die Spaltenbedingung auf, die dann in dem Chiffrierzylinder M-94 der U.S.Army und in den 1934 eingeführten Streifengeräten M-138 der amerikanischen Diplomaten und Militärs beachtet wurde.

Fehler durch Bequemlichkeit und Materialeinsparung

Die Erfinder von Chiffriersystemen und -maschinen zielen oft darauf ab, größere Bequemlichkeit in der Bedienung zu erzielen oder den Aufwand zu vermindern. Beides wurde von Willi Korn angestrebt, der 1926 die von Arthur Scherbius (1878–1929) 1919 zum Patent angemeldete Rotor-Chiffriermaschine ENIGMA (Abb. 1) zu verbessern versuchte. Die kommerzielle ENIGMA B chiffrierte durch Hintereinanderschaltung von 4 Rotoren. Korn führte in der ENIGMA C an Stelle des vierten Rotors eine Umkehrscheibe ein und machte die Zeitgenosssen — auch die Verantwortlichen in der Reichswehr — glauben, daß durch drei Rotoren auf dem Hinweg und drei auf dem Rückweg eine weniger angreifbare Chiffrierung entstünde. Überdies war die Chiffrierung nun selbst-reziprok[5], war eine Involution (Abb. 2b): Ging etwa **e** in **M** über, so ging auch **m** in **E** über. Es war also beim Übergang von der Chiffrierung zur Dechiffrierung kein Umschalten erforderlich. Diese Bequemlichkeit war überzeugend und bedeutete auch eine Materialeinsparung.

Die Tücke der *complication illusoire*

Schlaue Ideen müssen nicht ausschließlich der Bequemlichkeit und Materialeinsparung dienen. Sie können auch in der besten Absicht entstehen, die Chiffrierung durch Komplikation schwerer angreifbar zu machen. Dabei besteht die Gefahr, daß eine äußerliche Komplikation nur der Selbsttäuschung des Erfinders dient, nämlich dem Entzifferer gar keine zusätzlichen Schwierigkeiten bringt — das ist der harmlose Fall —, oder im schlimmsten Fall es ihm noch erleichtert.

Der von Korn angepriesene Hin- und Rückweg durch die Rotoren schien ein Musterbeispiel für eine nur scheinbare Komplikation, eine *complication illusoire* der harmlosen Art zu sein. Tatsächlich war er sogar tückisch: Er eröffnete einen bequemen Weg, die möglichen Lagen eines wahrscheinlichen Wortes zu finden. Es wurde nun nämlich kein Zeichen mehr durch sich selbst chiffriert, es gab keine Fixpunkte der Chiffrierung. Das brachte, worauf wir sogleich zurückkommen werden, eine bequeme Einbruchsmöglichkeit.

[5] Die Briten nannten die ENIGMA C deshalb 'Reciprocal ENIGMA'.

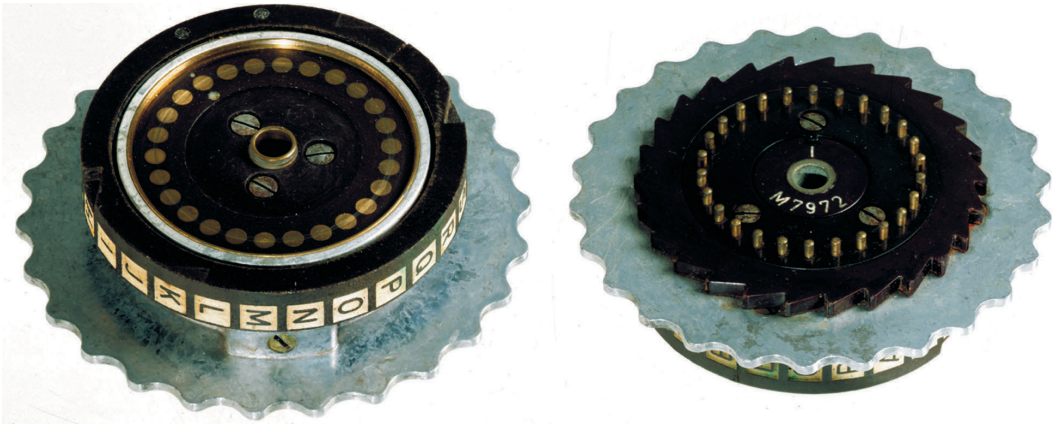

Abb. 1. ENIGMA-Rotor (Vorderseite und Rückseite).

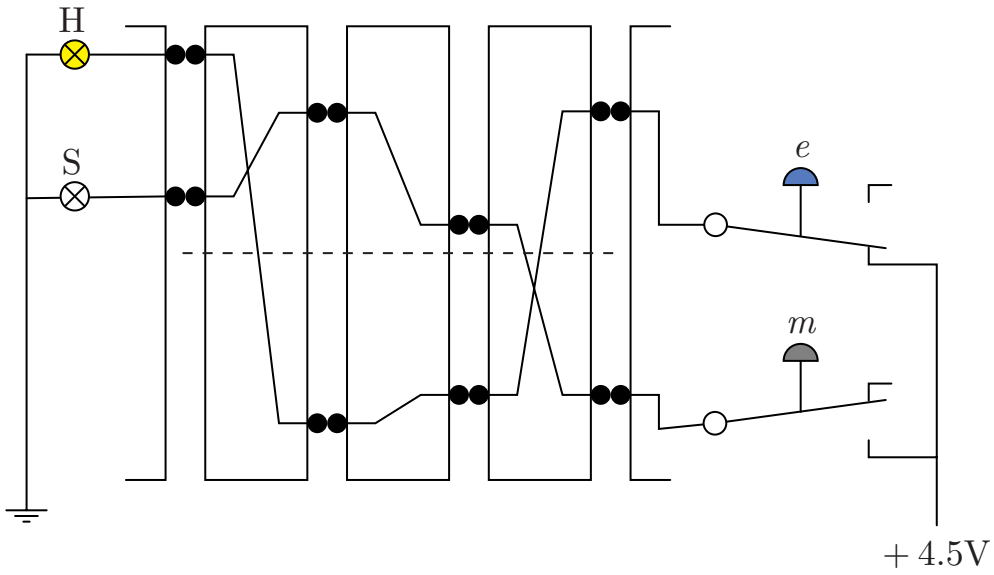

Abb. 2a. Stromlauf durch drei Rotoren: bei gedrückter Taste e leuchtendes Lämpchen H .

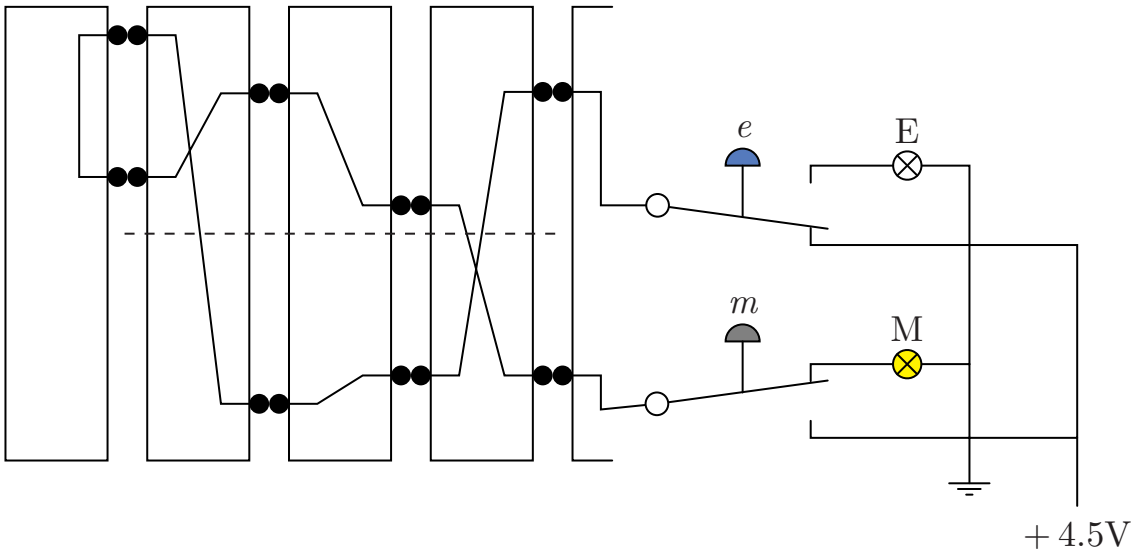

Abb. 2b. Stromlauf durch drei Rotoren und Umkehrscheibe ()
bei gedrückter Taste e leuchtet M, bei m leuchtet E .

Diese Schwachstelle zeigen neben der ENIGMA und ihren Verwandten auch andere Verfahren und Maschinen, beispielsweise die Chiffrierzylinder und die Streifengeräte: auch bei ihnen geht niemals ein Buchstabe in sich über. Damit wird jedoch ein Ausschließungsverfahren (Abb. 3) für die Lage einer vermuteten Phrase ermöglicht, das bei hinlänglich langer Phrase und bei Kenntnis der ungefähren Lage (etwa am Anfang oder am Ende) den Aufwand auf das Durchprobieren vergleichsweise weniger Lagen reduziert. Der fixpunktfreie Charakter der selbst-reziproken ENIGMA-Chiffrierung nach der Kornschen Idee war also eine *complication illusoire* der nicht mehr harmlosen Art — eine, die dem unbefugten Dechiffrierer sogar half.

```
Y O A Q U T H N C H W S Y T I W H T O J Q M T C F K U S L Z V S M F N G T D U Q N Y A V
e r l o s c h e n i s t l e u c h t t o n n e
  e r l o s c h e n i s t l e u c h t t o n n e
    e r l o s c h e n i s t l e u c h t t o n n e
      e r l o s c h e n i s t l e u c h t t o n n e
        e r l o s c h e n i s t l e u c h t t o n n e
          e r l o s c h e n i s t l e u c h t t o n n e
            e r l o s c h e n i s t l e u c h t t o n n e
              e r l o s c h e n i s t l e u c h t t o n n e
                e r l o s c h e n i s t l e u c h t t o n n e
          →       e r l o s c h e n i s t l e u c h t t o n n e
                    e r l o s c h e n i s t l e u c h t t o n n e
                      e r l o s c h e n i s t l e u c h t t o n n e
                        e r l o s c h e n i s t l e u c h t t o n n e
                          e r l o s c h e n i s t l e u c h t t o n n e
                            e r l o s c h e n i s t l e u c h t t o n n e
                              e r l o s c h e n i s t l e u c h t t o n n e
                                e r l o s c h e n i s t l e u c h t t o n n e
                                  e r l o s c h e n i s t l e u c h t t o n n e
                                    e r l o s c h e n i s t l e u c h t t o n n e
                                      e r l o s c h e n i s t l e u c h t t o n n e
                                        e r l o s c h e n i s t l e u c h t t o n n e
                                          e r l o s c h e n i s t l e u c h t t o n n e
```

Abb. 3. Ausschließung der Lage eines wahrscheinlichen Wortes bei fixpunktfreier selbst-reziproker Chiffrierung. Nur in der durch einen Pfeil bezeichneten Lage kann sich das Klartextwort befinden.

Die Erfindung Korns von 1926 (DRP 452 194) ging in die spätere Wehrmachts-ENIGMA ein, die aus der ENIGMA G ab 1928 von der Reichswehr als ENIGMA I entwickelt wurde. Sie stellte sich als deren bedeutendste Schwachstelle heraus, weil sie die mechanische ENIGMA-Entzifferung der Briten in Bletchley Park durch die sogenannten 'Turing-Bomben' beträchtlich erleichterte und den Aufwand abkürzte. Die Kryptologen der Wehrmacht erkannten die Schwachstelle bei der Einführung der ENIGMA I (römisch I) am 1. Juni 1930 nicht.

Die Briten, die die kommerzielle deutsche ENIGMA studiert hatten, fielen scheinbar ebenfalls auf die angeblich schlaue Idee von Korn herein: ihre TYPEX, 1926–1935 unter der Aufsicht einer Regierungskommission entwickelt und seit 1939 für das britische Heer und die Luftwaffe eingeführt, verzichtete nicht auf die Umkehrscheibe. Hingegen war die Fortschaltung der Rotoren bedeutend unregelmäßiger als die der ENIGMA, die nach Art eines Schrittzählers funktionierte.

Weiterhin verblieb ein kleiner, aber wesentlicher Unterschied zwischen der zivilen ENIGMA und den militärischen Typen: die ENIGMA I und natürlich auch die Wehrmacht-ENIGMA war mit einem 'Steckerbrett' (Abb. 4) versehen, das am Eingang in die Rotoren und am Ausgang aus den Rotoren wirksam war. Die Idee war bahnbrechend und fand Nachahmung auch bei den Briten. Ganz unnötigerweise war jedoch das Steckerbrett der Wehrmacht-ENIGMA ebenfalls eine fixpunktfreie Involution, was nur eine Bequemlichkeit in der Durchführung des täglichen Wechsels der Steckerverbindung mit sich brachte; sie ermöglichte aber insbesondere das raffinierte '*diagonal board*', das Gordon Welchman für die 'Turing-Welchman-Bomben' ersann.

Die TYPEX (Abb. 5) hingegen, die eine dem Steckerbrett entsprechende Zeichensubstitution durch zwei feststehende Rotoren hatte, verzichtete auf die fixpunktfreie, selbst-reziproke Eigenschaft der zusätzlichen Substitution. Tatsächlich entwickelte die deutsche Seite spät, gegen Ende des Krieges einen Zusatz (irrreführenderweise „Uhr") genannt), der einen raschen Wechsel der Steckerverbindung ermöglichte und dabei für 30 der 40 Einstellmöglichkeiten den selbst-reziproken

Charakter der Steckerverbindung aufgab. Welchman: *Non-reciprocal steckering demolished the principle of the diagonal board of a bombe*[6]. Das kam viel zu spät, um dem Desaster deskompletten Einbruchs der Briten in den ENIGMA-Verkehr zu entgehen. Hatten die Deutschen zuletzt doch Wind bekommen von dem best gehüteten, ULTRA genannten Geheimnis der Alliierten?

Abb. 4. 4-Rotor ENIGMA der Kriegsmarine, mit zweipoligem 'Steckerbrett' auf der Vorderseite. Einstellräder der 4 Rotoren im oberen Teil.

Die Briten ersetzten bei der Simulation der ENIGMA in den Turing-Bomben den Kranz von Rotorkontakten durch zwei Kränze: einen für den Hinweg, einen für den Rückweg (Welchman: *Two concentric circles of twenty-six terminals, instead of one circle*[7]) und zeigten damit, wie es die Deutschen hätten machen sollen: daß nämlich eine ENIGMA mit Umkehrscheibe möglich war, deren selbstreziproke Chiffrierung nicht fixpunktfrei war. Welchman: *It would also have been possible, though more difficult, to have designed an Enigma-like machine with the self-encipherment feature, which would have knocked out much of our methodology*[8]. Hätte die deutsche Seite den Materialaufwand nicht gescheut, den die Verdopplung der Kontaktanzahl und der 26-polige Umschalter 'Chiffrieren/Dechiffrierern' mit sich bringen würde, wäre eine ENIGMA entstanden, die die gefährliche Schwachstelle vermieden hätte.

Viele weitere Beispiele der *complication illusoire* ließen sich anführen, darunter beim kaiserlichen Heer im November 1914 die Ersetzung einer sogenannten doppelten Spaltentransposition durch eine polyalphabetische Substitution nach einer Art, die schon von Trithemius und Vigenère im

[6] Gordon Welchman, a.a.O. p. 137.
[7] Gordon Welchman, a.a.O. p. 236.
[8] Gordon Welchman, a.a.O. p. 168.

Abb. 5. Britische Chiffriermaschine Typex Mark III .

16. Jahrhundert eingeführt worden war, mit nachfolgender einfacher Spaltentransposition — die Franzosen waren entzückt. Oder, um nochmals auf die ENIGMA zurückzukommen, die Tatsache, daß bei den Rotoren I bis V der ENIGMA die Übertragsnuten jeweils an einer anderen Stelle angebracht waren: das sollte eine Erschwerung sein, bewirkte aber, daß sich herausfinden ließ, welcher Rotor als der „schnelle Rotor“ (der sich bei jedem Schritt bewegte) verwendet war; bei den Rotoren VI bis VIII der Marine, die später in Gebrauch kamen, stimmten dann die Lagen der Übertragsnuten überein. Man hatte wohl die Einbruchsmöglichkeit bemerkt — die Rotoren I bis V verwendete man trotzdem weiter.

Oder, um ein ganz modernes Beispiel zu nehmen: bei gewissen Chiffrierverfahren, bei denen Primzahlen eine Rolle spielen, werden „aus guten Gründen“ vorzugsweise sogenannte „sichere Primzahlen“[9] genommen — Primzahlen p derart daß auch $p' = \frac{p-1}{2}$ eine Primzahl ist, oder sogar „doppelt sichere Primzahlen“— Primzahlen p derart daß neben $p' = \frac{p-1}{2}$ auch $p'' = \frac{p'-1}{2} = \frac{p-3}{4}$ eine Primzahl ist (beispielsweise $p = 47,\quad p' = 23,\quad p'' = 11$). Da doppelt sichere große Primzahlen eine ziemliche Seltenheit sind und ihre Durchmusterung somit leichter fällt, könnte diese Komplikation auch ins Auge gehen. Auch bei Bazeries Chiffrierzylinder und bei den Streifengeräten denkt der Unerfahrene möglicherweise daran, daß die willkürliche Auswahl eines Chiffrates aus 25 möglichen die unberufene Entzifferung unheimlich erschwert, tatsächlich stellt sich das als grundlos heraus.

[9] Friedrich L. Bauer, *Decrypted Secrets*. Berlin und Heidelberg, Springer Verlag 2007 ; pp. 183, 207 .

Perfekte Sicherheit und praktische Sicherheit

Bei manchen „sensitiven“ Nachrichten, wie etwa auf militärischem Gebiet einem Angriffsbefehl, entfällt der Grund zur Geheimhaltung nach wenigen Stunden oder Tagen, bei anderen, insbesondere auf dem Feld der Politik und Diplomatie, wird man auch nach Jahrzehnten noch keine Aufdeckung wünschen. Der für die Sicherheit der eigenen Verfahren Verantwortliche muß demnach eine Abwägung treffen, welcher Aufwand erforderlich scheint, um die gewünschte praktische Sicherheit über eine ausreichend lange Zeit zu gewährleisten. Auf perfekte Sicherheit kann oft verzichtet werden und selbst wo sie angezeigt wäre, können praktische Schwierigkeiten, wie etwa der gedeckte Austausch individueller Schlüssel, dem entgegenstehen.

Bei Chiffrierverfahren, die nicht beweisbar sicher sind, besteht ein Problem darin, daß zwar immer mathematisch zuverlässige obere Schranken für den Aufwand zum Einbruch vorliegen — der ‘*brute force*’-Angriff des Durchprobierens aller (nämlich endlich vieler) Möglichkeiten liefert sie. In aller Regel geht es jedoch mit Einsatz von Köpfchen erheblich schneller, weswegen die von interessierter Seite oft angeführten kombinatorischen Komplexitäten — für die 3-Rotor-ENIGMA ein Viertel einer Quadrillion[10] — höchstens dazu dienen können, einen naiven Angreifer abzuschrecken und den Oberbefehlshaber in Sicherheit zu wiegen. Was man bräuchte, sind untere Schranken, d.h. Abschätzungen für den Mindestaufwand zum Einbruch. Gute solche Schranken in hinreichender Allgemeinheit kann man mathematisch nicht herleiten, man ist auf Empirie angewiesen und kann immer wieder überrascht werden durch einen Einbruch, der weniger Aufwand erfordert als man bisher gewöhnt war. Das macht das Spiel mit der Kryptanalyse so spannend.

Perfekte Sicherheit erzielt man mit beweisbar sicheren Verfahren. Bekannt ist die Verwendung einer einzigen unendlichen echten Zufallsfolge von Substitutionen (‘*one-time pad*’), wobei es schon genügt die Nachricht binär durch **0** und **1** zu codieren und lediglich die zwei Substitutionen Identität (**0**↦**0**, **1**↦**1**), realisiert durch Binäraddition von **0** und Spiegelung (**0**↦**1**, **1**↦**0**), realisiert durch Binäraddition von **1**, zu verwenden. Die *crux* der Angelegenheit besteht darin, sauber zu definieren was eine unendliche echte Zufallsfolge von Identität und Spiegelung, d.h. von **0** und **1**, sein soll. Akzeptiert ist heute, auf A. N. Kolmogorov zurückgreifend, die 1974 von Gregory J. Chaitin gegebene Definition — in der Fassung von Claus-Peter Schnorr

> *Für jede endliche Teilfolge der Zufallsfolge gibt es keine kürzere algorithmische Beschreibung als die Auflistung der Teilfolge — keine Teilfolge ist in eine kürzere Beschreibung ‚komprimierbar‘.*

Damit scheiden für unbrechbare Chiffrierungen alle unendlichen Ziffernfolgen aus, die durch einen festen, mit endlich vielen Zeichen aufgeschriebenen Algorithmus, also maschinell, erzeugt werden. Es nützt also nichts, einen solchen Algorithmus bei der Chiffrierstelle und bei der Dechiffrierstelle zu hinterlegen. Die Ziffernfolge (der „Schlüssel“) muß individuell sein, die Schlüsselvereinbarung muß streng genommen durch physikalischen Transport einer Kopie zur Chiffrierstelle und einer Kopie zur Dechiffrierstelle erfolgen — wobei keine weiteren Kopien für anderweitige Verwendung gezogen werden dürfen. Diese Erschwerungen machen es begreiflich, warum immer wieder die eigentlich striktest verbotene Mehrfachverwendung angeblich individueller Schlüssel vorkam — so bei den Sowjets, was den Amerikanern nach dem Ende des 2. Weltkriegs in jahrelanger unermüdlicher maschineller Arbeit den Einbruch in das höchste sowjetische Chiffriersystem (‘VENONA breaks’) gestattete.

Diese strenge Forderung der beweisbar sicheren Chiffrierung zu erfüllen, wurde in der Geschichte der Kryptographie tatsächlich gelegentlich, wo es auf perfekte Sicherheit ankam, ernsthaft versucht, so schon 1943 in Großbritannien mit ROCKEX-Maschinen bei der Übermittlung entzifferter ENIGMA-Nachrichten oder in den USA ab Mitte 1944 mit SIGTOT-Maschinen auf dem Heißen Draht zwischen Stalin und Roosevelt. Da Algorithmen zur Herstellung echter Zufallsfolgen ausscheiden, können bestenfalls physikalische Effekte, wie Röhrenrauschen, verwendet werden. Dabei war keineswegs immer sichergestellt, daß die theoretischen Anforderungen erfüllt waren. Manche solcher angeblichen Zufallsfolgen wurden sogar „nach Gefühl“ von Hand getippt, andere durch Maschinen, die eine sehr lange Periode hatten, erzeugt, wodurch sie garantiert ungeeignet waren.

Fehlerhafte Chiffriervorschriften

Gelegentlich führen auch Dienstvorschriften und Gewohnheiten zu Schwachstellen. Beim Gebrauch der deutschen ENIGMA war es üblich, Interpunktionen durch Buchstaben auszudrücken; der Punkt

[10] Periode der Rotorstellungen 16900, Permutationen der Rotoren 6, Verstellungen der Sperringe 17576, Steckerverbindungen bei 10 Steckern $150738274937250 \approx 1.5 \cdot 10^{14}$, insgesamt $2686467183181265484000000 \approx 2.7 \cdot 10^{23}$ Möglichkeiten.

und auch der Zwischenraum wurde durch *x* codiert. Damit wurde das *x* zum häufigsten Buchstaben, häufiger noch als das *e*. Der polnische Mathematiker Marian Rejewski (1905–1980), für das *Biuro Szyfrów* arbeitend, fand schon 1932 heraus, daß die meisten Klartexte mit /anx/ begannen. Diese Dreiergruppe, an fester Stelle stehend, reichte gerade aus, um die Anfangsstellungen der drei Rotoren zu bestimmen.

Auf der deutschen Seite herrschte auch eine Verdopplungsmanie: Wichtige oder für wichtig gehaltene Worte wurden verdoppelt: vonvon, anan; eilige Nachrichten begannen mit krkr (kr steht für 'Kriegstelegramm'). Besondere Ehrfurcht wurde gar durch Verdreifachung bezeugt: bduuu für Befehlshaber der U-Boote, okmmm für Oberkommando der Marine. Schon Porta hatte 1563 geraten, Buchstabenverdopplungen zu vermeiden und generell absichtliche Buchstabierfehler zu machen, „lieber als Dummkopf dazustehen, als den Preis für die Aufdeckung der Geheimnisse zu bezahlen".

Zahlen wurden, wenn sie mit Worten ausgeschrieben wurden, von y.....y eingerahmt, ebenso Eigennamen. Auch sie wurden verdoppelt: ysiebenyysiebeny — für die polnischen und britischen Kryptanalysten ein wahres Vergnügen. Die Verdopplung, die den technischen Grund hatte, im störungsanfälligen Morse-Funkverkehr eine Sicherung zu geben, wurde gedankenlos angewendet und hatte eine viel schlimmere Konsequenz: den Einbruch in das Kryptosystem.

Das Hauptproblem aller Chiffriermaschinen ist die Schlüsselvereinbarung. Sie kann in einer Dienstvorschrift für ein Nachrichtennetz von vornherein etwa für eine Woche, einen Monat vorgenommen werden, im täglichen oder gar stündlichen Wechsel. Dabei ist für die ENIGMA neben der Rotorlage, den Steckerverbindungen und den Ringstellungen auch die Anfangseinstellung der Rotoren für die jeweilige Nachricht festzulegen. Schon bei der kommerziellen ENIGMA wurde dabei abgeraten, mehrmals die selbe Anfangseinstellung der Rotoren zu benutzen, weil dadurch eine sehr einfache Einbruchsmöglichkeit entsteht: die einzelnen Chiffrate sind mit dem gleichen Schlüssel chiffriert, schon bei einem halben Dutzend solcher phasengleich chiffrierter Nachrichten ist die Entzifferung in der Regel ein Kinderspiel.

Es muß also für jede Nachricht eine eigene Anfangseinstellung („Spruchschlüssel") der drei Rotoren benutzt werden. Ein schlauer Mitarbeiter von Scherbius, möglicherweise sein Mitarbeiter Paul Bernstein, hatte die Idee, diese durch drei Buchstaben in einer Präambel zu übermitteln, natürlich nicht offen. Wie aber sollte sie chiffriert werden? Man hätte zu diesem Zweck eine eigene, von Zeit zu Zeit wechselnde Chiffriertabelle verwenden sollen (wie es die Kriegsmarine ab Mai 1937 für die 3-Rotor-ENIGMA, ab Februar 1942 für die 4-Rotor-ENIGMA mit einer Bigramm-Überchiffrierung tatsächlich vorschrieb). Aber Heer und Luftwaffe machten es sich einfach: man hatte ja die ENIGMA, die man ohnehin für unbezwingbar hielt, und so beging die Reichswehrführung schon 1930 den gravierenden Fehler, lediglich unter Benutzung der selben ENIGMA den Spruchschlüssel mit einer allgemeinen, länger gültigen Grundstellung zu chiffrieren.

War das schon eine Dummheit, so führte die deutsche Verdoppelungsmanie nun zur Katastrophe: da man mit gewissem Recht fürchtete, den chiffrierten 3-Buchstaben-Spruchschlüssel doppelt zu übertragen, denn das würde seinen Charakter ziemlich offenlegen, verdoppelte man den Spruchschlüssel im Klartext und chiffrierte diese 6-Buchstaben-Gruppe. Damit war an fester Stelle im Chiffrat eine 3-Buchstaben-Wiederholung vorgeschrieben, eine schier unglaubliche wahnwitzige Torheit — das erste, was das polnische *Biuro Szyfrów* 1932 durch Standard-Tests herausfand, war, daß die ersten sechs Buchstaben eines jeden aufgefangenen Funkspruchs eine innere Gesetzmäßigkeit aufwiesen, somit möglicherweise den chiffrierten verdoppelten Spruchschlüssel umfaßten. Diese Gesetzmäßigkeit genau herauszufinden, wurde 1932 dem jungen Rejewski aufgetragen, und unter der Annahme, daß die deutschen Nachrichtensoldaten für den Spruchschlüssel gewisse Buchstaben-Wiederholungen wie 'aaa' oder geläufige Buchstaben-Kombinationen auf der Tastatur, wie 'qwe', 'asd' bevorzugten, gelang ihm die Lösung[11] des ersten Rätsels der ENIGMA. Schritt für Schritt kämpfte sich Rejewski nach diesem Anfangserfolg, unterstützt von seinen Kameraden Henryk Zygalski (1907–1978) und Jerzy Różycki (1909–1942), durch das Gestrüpp der ENIGMA-Chiffrierung. Różycki half 1933 die Verdrahtung aller drei bis dahin benutzten Rotoren aufzudecken, Zygalski half, einen Katalog aufzustellen, aus dem unabhängig von der Steckerverbindung die Grundstellung abgelesen werden konnte — wobei sie von der deutschen Seite durch halbherzige kleine Verbesserungsschritte geradezu eine Erziehungsbeihilfe bekamen. Die Spruchschlüsselverdopplung wurde

[11] Marian Rejewski, in: Wladyslaw Kozaczuk. ENIGMA. University Publications of Amerika, Frederick, Md. 1985; pp. 241–271.

erst am 1. Mai 1940 fallen gelassen. Dies konnte tatsächlich geschehen, ohne daß es im Funkverkehr zu den befürchteten Problemen führte.

Bis 1938 hatten die polnischen Mathematiker vollen Einblick erreicht, dann wurde die weitere Arbeit erschwert durch eine Änderung in der Schlüsselvereinbarung und die Einführung zweier zusätzlicher Rotoren, die erforderte, statt bisher 6 nunmehr 60 Rotorordnungen durchzuprüfen. Die polnischen Mathematiker mechanisierten daraufhin die Dechiffrierung durch Bau einer Maschine, der *bomba*, und durch Benutzung der Zygalski-Lochblätter. Nach dem Einmarsch der Wehrmacht in Polen flüchteten sie. Rejewski und Zygalski konnten ihre kryptanalytische Arbeit schließlich in England fortsetzen, Różycki fand 1942 bei einem Schiffsunglück den Tod.

Für die Kryptanalyse gilt die Maxime: aus kleinen Erfolgen werden oft größere Erfolge ('*success breads further success*'). Am schwierigsten, wenn es einem die gegnerische Seite nicht allzuleicht macht, ist fast immer der Einstieg. Daß die Deutschen Fehler machten, schmälert nicht die Leistung der Polen: Franzosen wie Briten, anerkannt führend in der Kryptologie ihrer Zeit, mühten sich schon 1932 und noch 1938 vergeblich, die ENIGMA zu bezwingen. Aber die jungen polnischen Mathematiker hatten gelernt, analytisch zu denken. 1938 begannen übrigens auch die Briten, Mathematiker einzusetzen: Alan Turing, Gordon Welchman, Max Newman, Alan Stripp, Jack Good, Rolf Noskwith und bald viele andere. Die Kryptologie entdeckte noch vor der Mitte des 20. Jahrhunderts die Nützlichkeit des Wechselspiels zwischen den vorher dominanten Philologen und den Mathematikern. In Deutschland wurde der Mathematik generell nicht genügend Bedeutung zugemessen: *„The application of mathematics to military problems was neglected in Hitler's Germany, certainly by comparison with England and the U.S."* (Hans Heilbronn). Erst 1941/42 begann man im OKW/Chi, die Sicherheit der eigenen Chiffrierverfahren mathematisch untersuchen zu lassen, wozu die Mathematiker Karl Stein (1913–2000), später Professor in München und Gisbert Hasenjäger (1919–2006), später Professor in Münster, herangeholt wurden.

CHIFFRIERFEHLER DURCH LEICHTSINN ODER FAULHEIT DER BENUTZER

Nicht alle Schwachstellen der Chiffrierung sind den Chiffrierverfahren oder Chiffriermaschinen sowie den Chiffriervorschriften anzulasten. Viel ärger, weil weniger gut kontrollierbar, sind Benutzerfehler. Das beginnt bei klassischen Handverfahren mit der Wahl der Schlüssel für polyalphabetische Chiffrierung. Die Geschichte der Kryptographie kennt viele Fälle, wo ein naheliegendes, zu Herzen gehendes oder den Patriotismus unterstreichendes Schlüsselwort verwendet wurde, mit dem Ergebnis, daß bloßes Erraten zum Ziel führt. Man kennt das auch heute bei der Wahl von Paßworten.

Eine systematische Betrachtung kennt drei Hauptfehler, die Benutzern, vor allem wenn sie unter Druck arbeiten müssen, häufig unterlaufen.

1. Das Chiffriersystem wird durch den zum Geheimtext gehörigen Klartext (oder einen Teil davon) kompromittiert (Klartext-Geheimtext-Kompromittierung).

Das sollte nicht vorkommen, es sei denn durch List und Tücke verschafft sich ein Dienst den Klartext — der Geheimtext kann natürlich abgehört werden. Es gibt zahlreiche wahre und sicher auch einige erfundene Geschichten hierzu, etwa die von dem japanischen Beamten, der dem amerikanischen Botschafter Joseph C. Grew ein Papier zusteckte mit der Bemerkung, ein Mitglied der japanischen Regierung möchte der U.S.Regierung eine Botschaft übermitteln, habe aber Angst, die Militärs könnten davon erfahren; die Botschaft sollte deshalb im geheimsten diplomatischen Code übermittelt werden. Geholfen hat es den Japanern wohl nicht, das Streifengerät M-138 der USA zu brechen. Ein beliebtes Muster ist es, politisch brisante Falschmeldungen in Tageszeitungen zu lancieren — dazu gibt es auch eine traurige Geschichte aus der Zeit der Dreyfus-Affäre. Noch einfacher ist es, wofür die Russen bekannt waren, eine Kopie des Klartextes zu stehlen oder zu rauben. Schließlich gibt es auch den nicht seltenen Fall, daß eine betriebliche Störung des Funkkanals oder des Empfangsgerätes die Dechiffrierung verhindert und man nichts besseres weiß als den Absender zu bitten, die Nachricht im Klartext nochmals zu übermitteln.

Eine genügend umfangreiche Klartext-Geheimtext-Kompromittierung gibt eine ganze Chiffriertabelle oder wesentliche Teile eines Codebuches preis, bei polyalphabetischer Verschlüsselung mit bekannter Maschine einen ganzen Schlüssel.

Im Prinzip nicht anders ist es, wenn man nur ein Bruchstück des Textes kennt: Die allgemeine Methode ist, wie schon erwähnt, die des vermutetenen Wortes oder der vermutetenen Phrase. Das Verfahren, das die Briten mit der Turing-Bombe anwendeten, liefert durch eine raffinierte Rückkopplungsschaltung die vermutliche Lage des Wortes oder der Phrase und erlaubt damit die

Aufdeckung des Schlüssels. Im 2. Weltkrieg lösten die Alliierten durch Angriffshandlungen Meldungen mit erwarteten Phrasen aus („Erloschen ist Leuchttonne“), sie nannten das mit britischem Humor ‘Gartenpflege’.

2. Das Chiffriersystem wird durch die Übertragung der Chiffrate ein und des selben Klartextes mit zwei verschiedenen Schlüsseln kompromittiert (Geheimtext-Geheimtext-Kompromittierung[12]).

Ihre Gefährlichkeit liegt darin begründet, daß sie so leicht übersehen wird. Warum sollte nicht ein Tagesbefehl in zwei verschiedenen Kenngruppen-Netzen mit verschiedenen Schlüsseln übertragen werden? Wie Sir Harry Hinsley berichtete[13], kam dies durchaus vor, so am 14. März 1942, als Dönitz zum Admiral befördert worden war und diese Nachricht in identischer Fassung mit verschiedenen Schlüsseln chiffriert wurde, darunter denen des neuen Netzes SHARK (deutsch: Triton) der U-Boote und des bereits beherrschten Netzes DOLPHIN (deutsch: Hydra) der Überwasserschiffe. Technisch gesehen war auch die Spruchschlüsselverdopplung bei der ENIGMA eine Geheimtext-Geheimtext-Kompromittierung.

Im Jargon der britischen Entzifferungszentrale Bletchley Park hieß eine Geheimtext-Geheimtext-Kompromittierung ‘*a kiss*’. Besser hätte man das Entzücken darüber nicht ausdrücken können. Es rührte davon her, daß häufig ein bestimmtes Chiffrierverfahren schon gebrochen war und der ‘*kiss*’ zu einer höchst wünschenswerten Klartext-Geheimtext-Kompromittierung führte. So wurde häufig in neue Kenngruppennetze der ENIGMA-Marine-Chiffrierung mit Hilfe des gebrochenen ‘Werftschlüssels’ der kleinen Boote der Kriegsmarine oder des Wetterkurzschlüssels der Kriegsmarine eingedrungen.

Die Gefahr einer solchen Kompromittierung besteht auch, wenn Irrtümer beim Chiffrieren vorkommen. Sie machen zunächst dem befugten Dechiffrierer die Arbeit schwer, oft sogar unmöglich. Wird nun die ursprüngliche Nachricht mit einem anderen Schlüssel nochmals chiffriert, so besteht die Geheimtext-Geheimtext-Kompromittierung bis hin zur Stelle des Irrtums.

3. Das Chiffriersystem wird durch die Übertragung der Chiffrate zweier verschiedener Klartexte mit ein und dem selben Schlüssel kompromittiert (Klartext-Klartext-Kompromittierung).

Die Gefahr einer solchen Kompromittierung besteht, wenn Irrtümer beim Chiffrieren vorkommen, ebenfalls: Wird, anders als unter 2., die ursprüngliche Nachricht mit dem gleichen Schlüssel nochmals chiffriert, so erlaubt ein Vergleich der erst von der Stelle des Irrtums an verschiedenen Chiffrate durch eine Differentialanalyse’ gewisse Einblicke in das Verfahren. (Auf diese Weise wird auch das Innenleben von Chiffrierchips, die nicht zerstörungsfrei geöffnet werden können, untersuchbar.)

Was soll also ein Chiffrierer, der einen Schreibfehler gemacht hat, etwa eine ganze Zeile ausgelassen hat, machen? Die Originalnachricht darf überhaupt kein zweites Mal chiffriert werden — es bleibt also nichts anderes übrig als sie gründlich umzuformulieren. Das darf aber der Chiffrierer gar nicht auf eigene Faust tun. Also muß er seinem Vorgesetzten seinen Fehler eingestehen. Verständlich, daß er das möglichst vermeiden möchte. Kurz: die Kompromittierung ist unausrottbar.

Technisch gesehen, erlaubt die Klartext-Klartext-Kompromittierung einen Angriff, den schon 1883 Auguste Kerckhoffs (1835–1903) beschrieb und der als Superimposition bezeichnet wird: die bezüglich des Schlüssels phasenrichtige Überlagerung von etwa einem halben Dutzend oder mehr Chiffraten ergibt eine Reduktion auf eine Vielzahl monoalphabetischer Chiffrierungen, die Häufigkeitsbetrachtungen nahelegen.

Für eine bestimmte Art polyalphabetischer Chiffrierungen, die man[14] „Chiffrierungen mit einer kommutativen Schlüsselgruppe (*key group*)“ nennen kann, gelten Symmetriebeziehungen zwischen Schlüsseltextfolge und Geheimtext, die Kerckhoffs in einem Spezialfall *symétrie de position* genannt hat und die auch einen Rollenwechsel zwischen Klartext und Schlüssel gestatten. Damit können auch Häufigkeitsbetrachtungen für die Schlüsseltextfolge in die Kryptanalyse einbezogen werden, wenn, wie es häufig geschah, als Schlüsseltextfolge verständlicher Text vorlag. Man sollte also *key groups* vermeiden, Eleganz ist hier fehl am Platze.

In Spezialfällen kann nun sogar eine Superimposition von nur zwei Geheimtexten zum Einbruch führen, beispielsweise wenn die Schlüsselgruppe nicht nur kommutativ ist, sondern sogar durch

[12] eigentlich Schlüssel-Schlüssel-Kompromittzierung

[13] F. H. Hinsley, British Intelligence in the Second World War, Vol II (1981), Appendix 19, p. 749.

[14] Friedrich L. Bauer, *Decrypted Secrets*. Berlin und Heidelberg, Springer Verlag 2007 ; pp. 377–382 .

Additionen modulo 2 erzeugt wird. Dies war in natürlicher Weise der Fall bei einer bitweisen Chiffrierung, die Gilbert S. Vernam (1890–1960) im Jahre 1917 auf der Basis der 5-Bit-Fernschreibercodierung eingeführt hatte.

Ein geradezu klassischer Fall dieser Klartext-Klartext-Kompromittierung geschah am 30. August 1941 auf einer Funkverbindung Wien-Athen. Die britischen Horcher fanden zwei ungefähr gleichlange, rund 4000 Zeichen umfassende Funksignale in kurzem Abstand, die im Indikator HQIBPEXEZMUG der Länge 12 und in den ersten sieben Zeichen übereinstimmten — ein klarer Hinweis auf eine Korrektur mit unverändertem Schlüssel und auf eine Fernschreiberchiffrierung mit 12 Einstellrädern. Tatsächlich war noch während der Erprobung des Lorenz Schlüsselzusatzes (Abb. 6) SZ 40 (alias TUNNY bei den Briten) eine Störung aufgetreten, die zur Wiederholung und damit zur Kompromittierung führte. Die Nachricht wäre weder wichtig noch schützenswert gewesen und für die Erprobung wäre der Ersatz durch jede andere gerechtfertigt gewesen. Aber bei der Wiederholung wurde gleich zu Beginn statt /nummer/ abgekürzt /nr/ geschrieben.

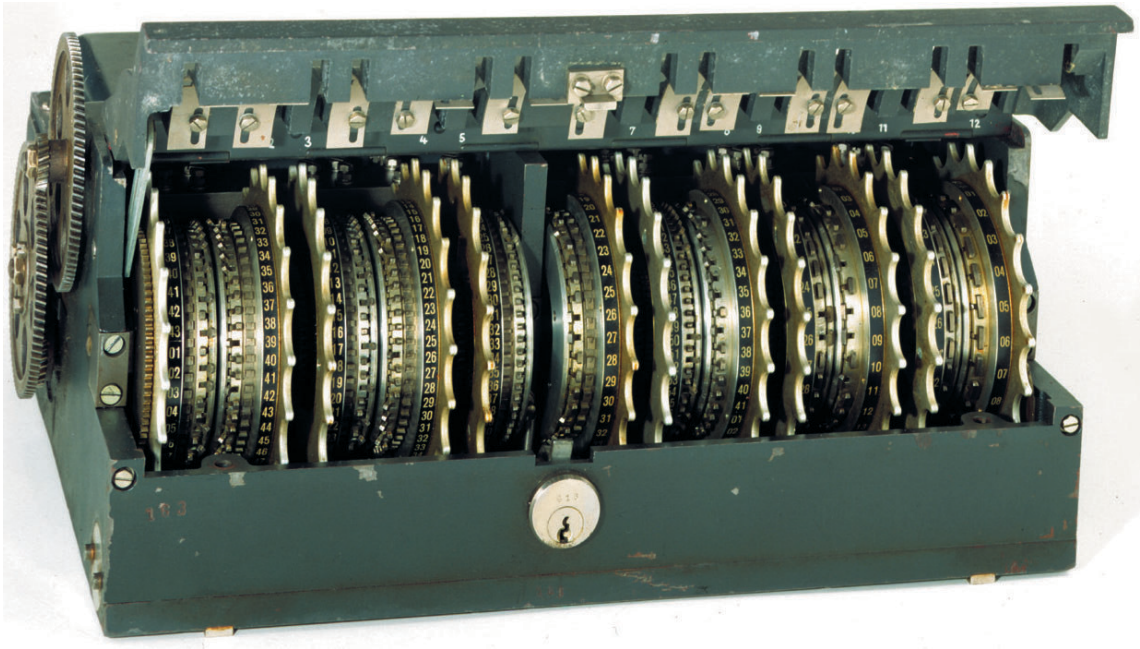

Abb. 6. Lorenz SZ 42 'Schlüsselzusatz' mit zwölf Chiffrierrädern.

Die schrecklichen Konsequenzen ihres Leichtsinns konnten die schlecht ausgebildeten Nachrichtensoldaten ja nicht ahnen: die Lösung, die dem britischen Oberst John H. Tiltman (1900–1984) in routinierter Handarbeit gelang, ergab eine Schlüsseltextfolge von 4000 Fernschreibzeichen und erlaubte dem jungen Mathematiker William Thomas Tutte (1917–2002), die mechanische Erzeugung des Schlüssels vollständig zu ergründen und damit ein ganzes System aufzuklären. Januar 1942 war alles bereit, um den bald einsetzenden Funk-Chiffrierfernschreiberverkehr zu brechen, wobei zunächst ein auf Ideen des Mathematikers Max Newman (1897–1984) beruhendes elektromechanisches Hilfsgerät, genannt ROBINSON, und bald ein schnelleres elektronisches, genannt COLOSSUS, die laufende Entzifferung beschleunigen halfen. COLOSSUS von Thomas H. Flowers (1905–1998), Sid Broadhurst, Bill Chandler und Allen Coombs, fertiggestellt Dezember 1943, war der erste elektronische Großrechner. 10 Geräte wurden nachgebaut, die verbesserte Version COLOSSUS Mark II kam gerade zu Beginn der Invasion zum Einsatz. Die Briten waren damit imstande, den Nachrichtenverkehr auf den wichtigsten deutschen Führungsebenen mitzulesen. Der Historiker Ralph Erskine[15] nannte diesen Einbruch "*The greatest cryptanalytical feat of World War II*", der insbesondere für den Verlauf der Landung in der Normandie entscheidend war.

Auch die Schweden waren erfolgreich, als sie 1940 eine deutsche Draht-Fernschreibverbindung anzapften, diesmal war es die Chiffrier-Fernschreibmaschine T52 von Siemens, im Jargon 'Geheimschreiber', die Arne Beurling (1905–1986) bezwang.

[15] In einem Interview mit Stephen Budianski.

NOCHMALS: SYSTEMBEDINGTE EINBRUCHSMÖGLICHKEITEN

Insbesondere für Fernschreib-Chiffriermaschinen, die nach Vernam mit binärer Codierung der Zeichen arbeiten, mag es naheliegen, die Menge der Chiffrierschritte eindeutig ('funktional') und umkehrbar eindeutig ('injektiv') den Schlüsselzeichen zuzuordnen; die Schlüsselzeichen bilden unter der Zusammensetzung eine *key group*. Das Kryptosystem ist dann *closed under composition*: für je zwei Schlüsselzeichen existiert in drittes derart daß es die Zusammensetzung der beiden ersteren bezeichnet. So elegant das aussehen mag — es vereinfacht jedenfalls den Chiffrier- und den Dechiffriervorgang — macht es auch den Einbruch in die Chiffrierung einfacher, was oft übersehen wurde.

Dabei lehrten schon um 1580 Giovanni Battista Argenti und sein Neffe Matteo Argenti den Gebrauch von Varianten ('Homophonen') bei der Chiffrierung, also die Preisgabe der eindeutigen Chiffrierung zum Zweck der Erschwerung der unbefugten Entzifferung, und dies wurde bis ins 20. Jahrhundert bei Hand-Chiffrierverfahren nicht vergessen — aber mit der Einführung von Maschinenchiffrierung glaubten die überheblichen Erfinder, diese Jahrhunderte alte Erfahrung nicht mehr berücksichtigen zu müssen.

Nun waren zwar die Schöpfer der seit 1938 entwickelten Chiffrierfernschreibmaschine Siemens & Halske T52 (britischer Deckname *Sturgeon*), August Jipp, Eberhard Hettler und Ehrhard Rossberg, die ein deutsches Patent von 1930 darauf hielten, keine ausgebufften Kryptologen, aber daß der sozusagen unter den Augen des OKW/Chi seit 1938 entwickelte Lorenz Schlüsselzusatz SZ 40 (alias TUNNY) nicht besser war, mag verwundern. Erich Hüttenhain, der im OKW/Chi die zuständige Abteilung IV (Analytische Kryptanalysis) leitete, fand vor dem Ausbruch des Krieges, daß „weder T52a/b noch SZ 40 den geltenden Sicherheitsansprüchen genügten" (Donald W. Davies)[16]. Die späteren Verbesserungen (T52c, T52e bzw. SZ 42) waren halbherzig und hielten jedenfalls die Erfolge der Briten nicht auf, der Gebrauch von Homophonen hätte auch eine radikale Umkonstruktion erfordert.

Nach Kriegsende fanden die Alliierten übrigens heraus, daß auf deutscher Seite in der Tat für den 1. Mai 1945 ein in Bletchley Park befürchteter Wechsel in den Vorschriften der Kriegsmarine für den Gebrauch der Bigramm-Überchiffrierung der ENIGMA geplant war, der alle existierenden kryptanalytischen Ansätze nutzlos gemacht hätte. Er wäre auch schon früher möglich gewesen.[17] Nunmehr kam jedoch auf deutscher Seite die Einsicht in die eigenen Schwächen allemal zu spät.

Ironie des Schicksals: Unterschätzung des Gegners

Sowohl bei der ENIGMA wie bei den Chiffrierfernschreibern hatte die deutsche militärische Führung nicht mit der Intelligenz auf der Seite der Polen, Briten und Schweden gerechnet. An guten Mathematikern gab es in Deutschland keinen Mangel, wenn auch einige der Besten unter Hitler das Weite suchten. Wohl aber standen, ganz im Gegensatz zu Frankreich, Mathematiker nicht in sehr hohem Ansehen. Die Chiffrierabteilung Chi des OKW wie auch die Funkentzifferungsdienste des Heeres, der Kriegsmarine und der Luftwaffe waren jedenfalls nicht rechtzeitig und nicht so stark mit Mathematikern versorgt worden, wie es bei den Alliierten der Fall war. Und die Luftwaffe des Banausen Göring funkte, was das Zeug hielt. Das Auswärtige Amt hingegen war viel vorsichtiger, verwendete weder ENIGMAs noch Chiffrierfernschreiber und mußte, so viel man weiß, kaum Niederlagen hinnehmen, hatte aber durch Rohrbach einen technisch bedeutsamen Erfolg gegen die Diplomatie der U.S.A., dessen Ausnutzung nur die Umstände — die Einführung von Chiffriermaschinen für ihre diplomatischen Kanäle — verhinderten.

Geheimhaltung und Authentizität im Konflikt

Wenn es in der klassischen Kryptologie als selbstverständlich galt, den Chiffrierschlüssel und den Dechiffrierschlüssel geheimzuhalten — sie konnten sogar, wie im Falle der ENIGMA — identisch sein, so gibt es seit 1976 eine Variante, die den Chiffrierschlüssel öffentlich macht — Voraussetzung ist natürlich, daß man aus dem Chiffrierschlüssel den Dechiffrierschlüssel nur unter unpraktikablen Anstrengungen gewinnen kann. Es gibt tatsächlich dafür geeignete schwer umkehrbare Funktionen ('Einweg-Funktionen' ist eine suggestive Übertreibung). Solche asymmetrische Chiffrierung besitzt notwendigerweise keine beweisbare perfekte Sicherheit. Sie hat aber organisatorische Vorteile, insbesondere bei großen Netzen. Und sie bietet den Nachrichtendiensten ein Betätigungsfeld.

---

[16] In: Donald W. Davies, *The Lorenz Cipher Machine SZ 42*, CRYPTOLOGIA XIX, p. 41.

[17] Ralph Erskine, *Ultra and Some U. S. Navy Carrier Operations*, CRYPTOLOGIA XIX, p. 95 Fußnote 52.

Eine Konsequenz dieser Chiffrierung mit öffentlichen Schlüsseln ist, daß dem Nachweis der Authentizität einer Nachricht weitaus höhere Bedeutung als bei der Chiffrierung mit geheimen Schlüsseln zukommt. Beides, Geheimhaltung und Authentisierung einer Nachricht läßt sich auch verbinden. Für die Sicherheit besteht aber dabei ein grundsätzlicher Konflikt. Dies sei an einem einfachen Beispiel erläutert: Um sicherzugehen, daß eine Nachricht mit Alarmcharakter nicht auf dem Übertragungsweg gespeichert und nach einiger Zeit wieder eingeschleust wird, empfiehlt es sich, in die Nachricht eine Zeitangabe aufzunehmen. Man muß allerdings dabei eine Klartext-Geheimtext-Kompromittierung in Kauf nehmen, die die Sicherheit der Geheimhaltung herabsetzt. Geheimhaltung und Authentisierung können sich also behindern: Chiffrierung ist gegen Brechen umso besser geschützt, je weniger Redundanz sie enthält, gegen Fälschung hingegen, je mehr Redundanz sie enthält. Der mittlere Weg erlaubt sowohl Brechen wie Fälschung.

CHIFFRIERFEHLER NOCH UND NOCH

Rohrbach schrieb: „Die Sicherheit von Maschinen ist nicht besser als ihr Gebrauch“. Boris Hagelin, der schwedische Erfinder und Erbauer der in den USA in Lizenz zu Hunderttausenden gefertigten M-209 kehrte es um: “*The quality of a machine depends largely on its use*”. In die bewußte oder unbewußte Verletzung von Sicherheitsvorschriften teilten sich in Deutschland Stabsoffiziere und Nachrichtensoldaten.

Ein im Ausland oft belächelter Hang der Deutschen zum Gebrauch von Titeln, Stereotypen, Routinewendungen führte zu einer Fülle von vermuteten Phrasen; wobei aus einem Erfolg oft der nächste erwuchs. Gestützt auf den Glauben an die Unbrechbarkeit der Chiffriermaschinen, unterzogen sich die Stabsoffiziere häufig nicht der Mühe, Ortsnamen, Namen von Flüssen und Bergen, Namen von Personen und Unterschriften durch Decknamen zu ersetzen; auch ließen sie textuelle Wiederholungen zu. Selbst in stereotypen Standardmeldungen wie „Keine besonderen Vorkommnisse“ wurden peinlich genaue Zeitangaben gemacht — besser wäre es gewesen, solche Meldungen überhaupt zu unterlassen oder, wenn es denn der Dienstbetrieb erforderte, in Klartext zu funken.

Die Nachrichtensoldaten waren nicht besser als ihre Ausbildung und ihre Ausbilder. Dienstvorschriften warnten oft nicht präzise genug vor unabsichtlichen Chiffrierfehlern oder waren mißverständlich. Als 1933 die häufige Wahl von Spruchschlüsseln wie ′aaa′ oder ′sss′ ausdrücklich verboten wurde, geschah das so, daß überhaupt keine Buchstabenwiederholungen in Spruchschlüsseln mehr gewagt werden konnten. Unverständlich war auch, daß niemals zwei nebeneinanderliegende Buchstaben auf dem Steckerbrett durch Stecker verbunden werden durften.

Zwei harmlos scheinende Unsitten der Soldaten der deutschen Luftnachrichtentruppe, von den Briten ‘Herivel tips’ und ‘Cillis’ genannt, traten 1939 in ENIGMA-chiffrierten Luftwaffensprüchen so häufig auf, daß sie von den Briten routinemäßig zum Brechen benutzt wurden: Der ‘*Herivel* tip’ besagte, daß nach Fixierung der Ringstellung die Rotoren nicht weitergedreht wurden und der im Klartext übertragene 3-Buchstaben-Indikator mit der Buchstabenkombination, die die Rotoren anzeigten, zusammenfiel. Dies legte die Ringstellung offen. ‘Cillis’ beruhten auf dem Gebrauch eigentümlicher gleicher Buchstaben-Muster auf der Tastatur für die Wahl des Indikators[18] und des Spruchschlüssels. Das ergab drei Buchstaben-Paarungen zwischen Klartext und Geheimtext. Insbesondere bei Sprüchen, die in Teile zerlegt waren, gelang so, bis es durch die Turing-Bomben überholt war, häufig der Einbruch. Eine dritte Unsitte, genannt ‘*Parkerismus*’, wurde von Bürokraten ausgelöst, die die monatlichen Schlüsselunterlagen für die ENIGMA-Netze herstellten: sie wiederholten nach geraumer Zeit die sämtlichen monatlichen Sequenzen von Ringstellungen, Rotorlagen und Steckerverbindungen. Die Briten brauchten, wenn ihnen an gewissen Tagen der Einbruch gelungen war, nur den gleichen Tag eines späteren Monats abzuwarten und zu probieren, ob die gleichen Daten wieder zum Erfolg führten.

Mangelnde Überwachung und andere Überheblichkeiten führen zum Ruin

Wie schon eingangs gesagt: Der schlimmste Feind sitzt im eigenen Boot — Ahnungslosigkeit, Überheblichkeit, ‘das Unbequeme nicht wahr haben wollen’.

Man kann nicht sagen, daß die deutsche Seite es an der Überwachung der Chiffriersicherheit gänzlich fehlen ließ; einige Änderungen wie die vom 15. September 1938 oder die vom 1. Mai 1940 können aber auch durch nachrichtendienstliche Erkenntnisse ausgelöst worden sein. Insgesamt war

[18] In der Chiffriervorschrift, die am 15. September 1938 in Kraft trat.

die Überwachung mangelhaft und entsprach damit der Überheblichkeit, der Krieg sei ohnehin schon (fast) gewonnen. Jedenfalls wurde auf deutscher Seite das Gespür für die Gründe der Vorschriften zur Chiffriersicherheit nicht genügend gepflegt. Gordon Welchman schrieb 1982: "*At any time during the war, enforcement of a few minor security measures could have defeated us completely*" und "*the* [Enigma] *machine as it was would have been impregnable if it had been used properly*". David Kahn bemerkte dazu: "*The Germans had no monopoly on cryptographic failure. In this respect the British were just as illogical as the Germans*". Er hätte auch hinzufügen können „die US-Amerikaner", denn ihr Verkehr mit den Hagelinschen Maschinen M-209 (Abb. 7) wurde vom B-Dienst der Kriegsmarine (der übrigens auch für lange Zeit bei der britischen Royal Navy, solange sie mit Codebüchern arbeitete, mitlas) regelmäßig gebrochen. Die US-Amerikaner ihrerseits brachen in den Verkehr der italienischen Marine mit Hagelin-Maschinen ein, und auch hier galt, wie der Historiker Ralph Erskine 1982 schrieb: "*Hagelin* [C-38m] *was virtually impregnable when used properly, as it was by Norway and Sweden*".

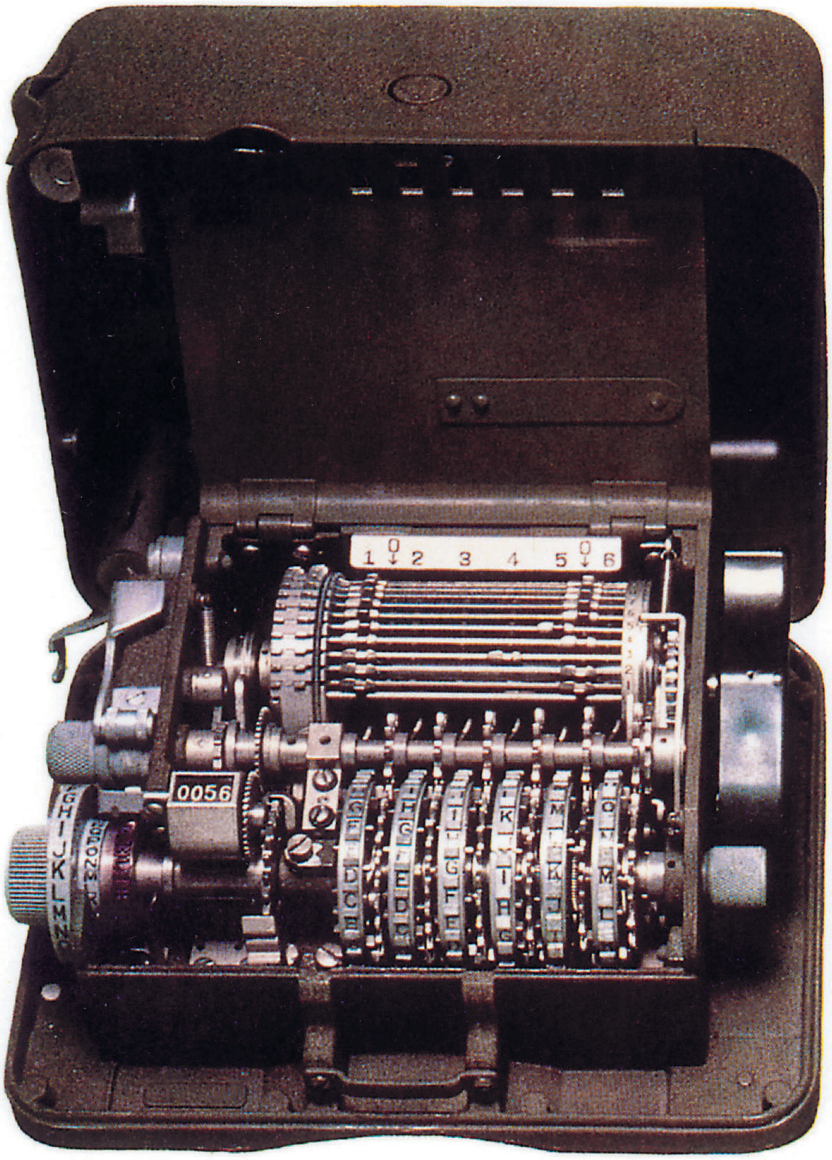

Abb. 7. US-amerikanische Chiffriermaschine M-209 (Hagelin C-36).

Es ging also auch anders. Die Maschine M-134 (SIGABA) des amerikanischen Militärs wurde allem Anschein nach niemals kompromittiert. Das spricht sowohl für die Qualität des Entwurfs, der unter der Kontrolle von Oberst Frank B. Rowlett (1908–1998) stand, wie für die Disziplin der Benutzer. "*The Germans ... wrote in the war diary of the codebreakers of Army Group C, that, because statistical tests showed that no breaks were possible, they had decided to stop even intercepting U.S. Army*

five letter (SIGABA) messages." (David Kahn)[19] Auf den Spuren von Rowlett arbeitete Seymour R. Cray (1928–1996), der 1976 den Supercomputer CRAY-1 (Abb. 8) mit hoher Parallelisierung für kryptanalytische Zwecke der US-amerikanischen Regierung (NSA) baute. Eine abgespeckte Version CRAY-1 S (1979) fand auch zivile Verwendung, ein Exemplar steht im Deutschen Museum. Nachfolgermodelle waren CRAY X–MP (1982) und schließlich 1996 CRAY T3E (1998: T3E-1200E, 2.4 teraflop/s).

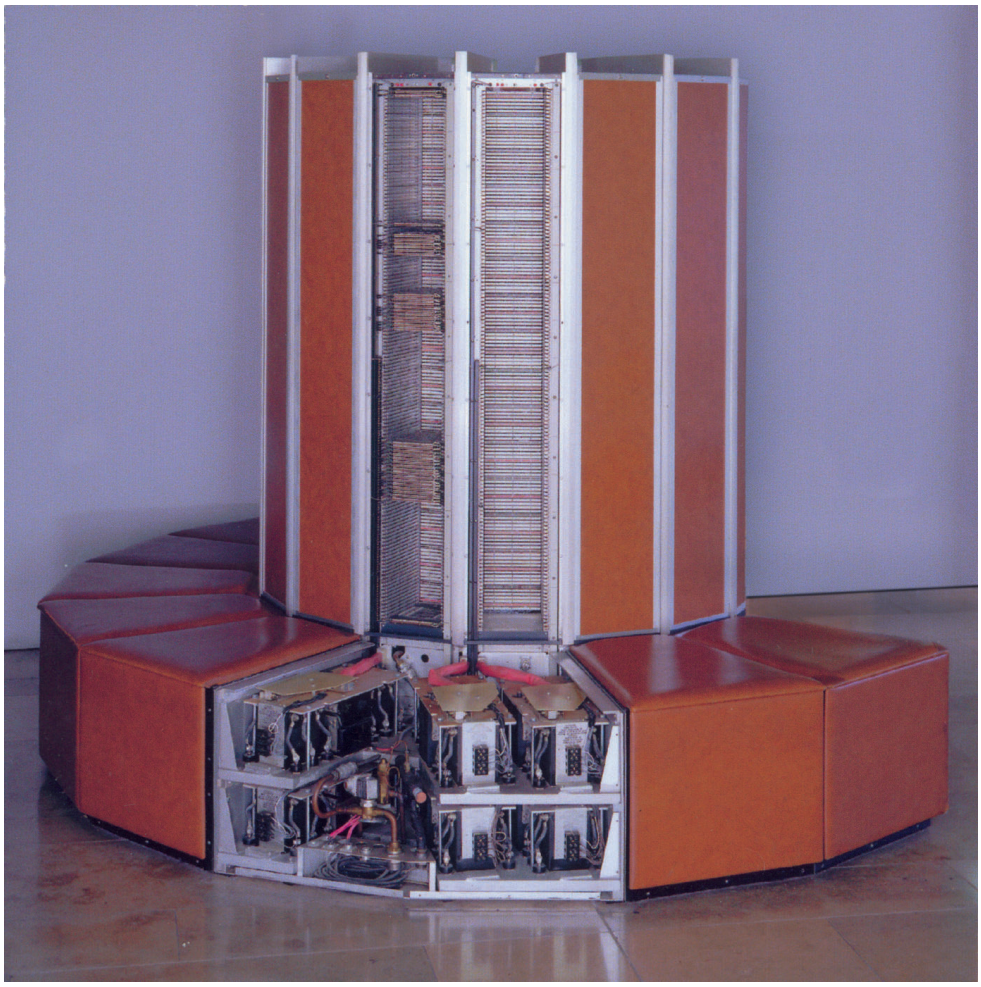

Abb. 8. Supercomputer CRAY-1 S,
aus einer militärischen Entwicklung für kryptanalytische Zwecke stammend.

NOCHMALS: DIE KOMÖDIE DER IRRUNGEN

Jedenfalls: Angesichts der Opfer an Menschen, die mit den aufgeführten Irrungen verbunden waren, sollte man wohl eher statt von einer Komödie von einer Tragikomödie der Irrungen in der Kryptologie sprechen.

Die allgemeine Schlußfolgerung für die Chiffrierbüros muß also sein, schon in Friedenszeiten dafür zu sorgen, daß Generäle und Botschafter nicht ignorant sind, daß genügend viele kryptologisch gut ausgebildete Stabsoffiziere und Nachrichtensoldaten, Botschaftssekretäre und Schreiber verfügbar sind, und daß die Überwachung auf allen Ebenen lückenlos ist.[20]

Vor Überraschungen wird man aber nie sicher sein. Étienne Bazeries drückte es 1901 so aus: "*En cryptographie, aucune règle n'est absolue*". Heute, mehr als 100 Jahre später, wird es nicht anders sein. Besser ist es allemal, auf geheimzuhaltende aggressive Aktionen zu verzichten. "*The Cold War in its present, miniature form has crept into the chips*".[21]

[19] In: Frank B. Rowlett, *The Story of Magic*. Aegean Park Press 1998. Epilogue pp. 249–258.
[20] Hoffentlich lesen einige der Verantwortlichen diese Zeilen.
[21] Friedrich L. Bauer, *Decrypted Secrets*, Berlin und Heidelberg, Springer Verlag 2007, S. 458.