1. Historisches

Am 6. Februar 1923 meldet ein gewisser Arthur Scherbius von der Chiffriermaschinen AG Berlin unter der Nummer 1657 411 in den USA ein Patent für ein Chiffriergerät an, welches den Namen Enigma (griech. ainissesthai: in Rätseln sprechen) trägt. Scherbius sucht vor allem zivile Käufer. In seinem Prospekt preist er die Enigma wie folgt an: »Die Neugier der Konkurrenten kann alsbald mit einer Maschine ausgeschaltet werden, die die Geheimhaltung Ihrer gesamten Korrespondenz und Ihrer Dokumente, zum mindesten der wichtigsten Akten, ohne allzu hohe Kosten gewährleistet. Ein einziges gut gehütetes Geheimnis schon gleicht die Ausgaben für den Ankauf der Maschine aus.» (Heute beträgt der Liebhaberwert für eine einfache Enigma zirka Fr. 3500.-.)

Versuchen wir uns kurz, die politische und wirtschaftliche Situation in Deutschland in dieser Zeit zu vergegenwärtigen: Das Deutschland der Weimarer Republik erlebt, dank amerikanischer Finanzhilfe, ein ungeahntes Wirtschaftswunder. An der Konferenz von Locarno akzeptiert der deutsche Aussenminister Stresemann den Status quo im Westen, denjenigen im Osten jedoch nur als Provisorium. Nur mit Mühe kann sich Stresemann mit seiner Politik der Verständigung gegen die immer stärker werdenden nationalistischen Kreise in Deutschland zur Wehr setzen, welche die berüchtigte Dolchstosslegende des im Feld unbesiegten Heeres, dem die Republikgründer angeblich meuchlings in den Rücken gefallen seien, vertreten. Nach Stresemanns Tod 1929 und als Folge der Weltwirtschaftskrise ziehen sich Ende der zwanziger Jahre immer stärker die Gewitterwolken des aufkeimenden Nationalsozialismus zusammen, welcher schliesslich zur Machtübernahme Hitlers am 30. Januar 1933 führt. Was nun kommt, ist nur allzu bekannt: Austritt Deutschlands aus dem Völkerbund, Besetzung des entmilitarisierten Rheinlandes, Einführung der allgemeinen Wehrpflicht, Anschluss Österreichs, Umwandlung der Tschechoslowakei ins »Reichsprotektorat Böhmen und Mähren», gleichzeitig Abessinienkrieg Italiens und spanischer Bürgerkrieg. Der englische Premierminister Chamberlain, welcher glaubt, Hitlers Territorialansprüche seien nun nach der Annexion von Österreich und der Tschechoslowakei befriedigt, unterschätzt mit seiner Appeasement-Politik die wahren Ziele Hitlers völlig, welcher systematisch auf Grund der in der deutschen Geschichte immer wieder herumgeisternden Idee der «Erweiterung des Lebensraumes der Germanen gegen Osten» einen neuen Weltkrieg vorbereitet. Der Polenfeldzug Deutschlands am 1. September 1939 führt endgültig zum Krieg.

Die Enigma verkauft sich anfangs nicht besonders gut, so dass sich Scherbius aus der Firma zurückzieht und das Unternehmen 1934 von Rudolf Heimsoeth und Elsbeth Rinke übernommen wird. Pech für Scherbius, denn nun erwerben Wehrmacht, SS, SD, Polizei, das Auswärtige Amt, sowie Japan, Italien und Spanien in den Jahren 1935 bis 1945 zusammen schätzungsweise etwa 200 000 Geräte, bei denen es sich um verschiedene Varianten der Enigma handelt. Sofort beginnen vor allem in Polen und Frankreich erste Versuche zum Knacken der Enigma-Chiffre. Später arbeiten auch die Engländer und die Amerikaner (gegen die von Japan benützten Enigma-Geräte) immer stärker mit. Berühmt geworden sind vor allem der englische Mathematiker Alan Turing (dessen Konzept eines Computers mit potentiell unendlichem Speicher [sog. «Turingmaschine»] später in der Theoretischen Informatik von grosser Bedeutung werden sollte), die drei polnischen Mathematiker Marian Rejewski, Jerzy Różycki und Henryk Zygalski und der französische Hauptmann Gustave Bertrand, welcher die kryptologische Zusammenarbeit Polens mit Frankreich organisiert und aufrechterhält (obwohl Frankreich 1939 seiner vertraglich festgelegten militärischen Beistandspflicht gegenüber Polen nicht nachkommt). Durch H.-T. Schmidt (Deckname «Asche», «H.E.»), einen jungen Mitarbeiter der Chiffrierstelle in der deutschen Reichswehr, werden dem französischen Geheimdienst in den Jahren 1932 bis 1934 sehr viele nützliche Dokumente und Informationen über die Enigma zugetragen. Die Dekryptierung (im Gegensatz zum Wort «Dechiffrierung» bedeutet «Dekryptierung» die «Dechiffrierung durch einen Unberechtigten») gelingt bald zu einem grossen Teil, und bereits im August 1939 können nahezu 90% der an Polens Westgrenze aufmarschierten Wehrmachteinheiten vom polnischen Generalstab erkundet werden. Allerdings nützon die Polen die in den dreissiger Jahren erhaltenen Informationen nicht in dem Mass, wie es die

Daniel Neuenschwander

Situation erfordern würde, auch sie lassen sich durch die in die Mode gekommene Appeasement-Politik einlullen und schliessen 1934 sogar einen Nichtangriffspakt mit Deutschland ab!

Selbstverständlich werden die von den Deutschen während des Krieges verwendete Militärversion der Enigma und die Schlüsselbefehle immer wieder verändert, so dass auf alliierter Seite stets mit der neuesten Entwicklung Schritt gehalten werden muss. Man gibt sich jeweils ausserordentliche Mühe, dem Gegner plausible «Gründe» für die erhaltene Information vorzuspiegeln, um ihn von seinem Vertrauen in die Enigma nicht abzubringen. Dies verfehlt seine Wirkung nicht, auf deutscher Seite wiegt man sich, was die kryptologische Sicherheit der Enigma anbetrifft, in absoluter Sicherheit. Das vielleicht tragischste Beispiel in diesem Zusammenhang ist die deutsche Bombardierung der englischen Stadt Coventry: Auf englischer Seite weiss man früh genug über die deutschen Absichten, so dass man die Stadt hätte evakuieren können. Churchill entscheidet aber für Stillschweigen und opfert so gewissermassen die Bevölkerung

von Coventry der Geheimhaltung über den Erfolg der kryptoanalytischen Angriffe auf die Enigma.

Nun zu einigen ausgewählten Ereignissen im Zweiten Weltkrieg, welche durch dekryptierte Enigma-Meldungen entscheidend beeinflusst worden sind:

- Bei der Kesselschlacht von Dünkirchen (1940) gelingt es den Engländern, 340 000 britische und französische Soldaten einzuschiffen, bevor die Deutschen den Ring um Dünkirchen schliessen können.
- Alle Operationen Hitlers gegen England erhalten stets den Decknamen «Seelöwe», was die Dekryptierung diesbezüglicher Texte dank eines «mot probable» wesentlich erleichtert! Andere häufig benutzte «mots probables» sind «Führerbefehl», «Heil Hitler», usw.
- Nachschubkonvois aus italienischen Häfen nach Nordafrika können gestoppt werden. Hier schöpft der deutsche General Kesselring in der Tat Verdacht auf ein Leck im Informationssystem, wird aber von Berlin «beruhigt», was wiederum den Alliierten zeigt, dass der deutsche Generalstab nach wie vor nichts von der gelungenen Attacke auf die Enigma weiss.
- Auch werden die alliierten Landungen in Marokko und Algerien 1942 und in der Normandie 1944 sowie ihre Besetzung Siziliens erleichtert.
- Ebenfalls bezüglich Entwicklung neuer Waffensysteme in Deutschland werden viele Informationen mit der Enigma verschlüsselt, die so von den Alliierten mitgelesen werden können.
- Bei der Schlacht bei den Midway-Inseln zählen die Japaner auf das Überraschungsmoment. Durch Mithören des japanischen Funkverkehrs kann aber der amerikanische General Chester Nimitz rechtzeitig Gegenmassnahmen einleiten. Bekanntlich bedeutet dieses Ereignis den Wendepunkt im amerikanisch-japanischen Krieg im Pazifik zugunsten der USA. Dass der Pazifikkrieg wesentlich durch die Entzifferung der Enigma-Funksprüche entschieden wird, beweist eindrücklich eine Briefstelle von General G. C. Marshall an Gouverneur T. E. Dewey: «Schon die Operation in der Korallensee basiert weitgehend auf entzifferten Funksprüchen; die wenigen Schiffe, die wir hatten, befanden sich zur richtigen Zeit am richtigen Ort. Wir konnten unsere begrenzten Kräfte konzentrieren und die Japaner an der Erobe rung der Midway-Inseln hindern; andernfalls wären wir etwa 3000 Meilen vom Angriffsziel entfernt gewesen. (...) Bei der Führung unserer Operation im Stillen Ozean stützten wir uns auf die verfügbaren Angaben über die Gruppierung der japanischen Kräfte und Mittel. Wir kennen die Stärke ihrer Truppen in den Garnisonen und ihre derzeitigen Vorräte an Kriegsgerät und Proviant und verfolgen, was sehr wichtig ist, die Bewegungen der japanischen Flotte und der Konvois. Die schweren Verluste, die unsere U-Boote den Japanern zufügen und von denen zuweilen die Presse berichtet, sind weitgehend dem Umstand zuzuschreiben, dass wir wissen, wann ihre Konvois auslaufen, wohin sie fahren, und somit unsere U-Boot-Kräfte informieren können, an welcher Stelle sie auf sie warten sollen.» Und über den Krieg in Europa steht im selben Brief: «Die wichtigste Quelle und Grundlage unserer Kenntnisse über die Absichten Hitlers in Europa ist die entzifferte Korrespondenz des japanischen Botschafters Hiroshi Oshima in Berlin. (...)»
- 1942 gelingt es den deutschen Kryptologen, den britischen Marinecode zu knacken. Dabei stellt sich heraus, dass der Gegner viele Daten über die Positionen deutscher Schiffe besitzt, trotzdem glaubt niemand an das Knacken des Enigma-Codes.

Abb. 1: Enigma.

Inwiefern das Knacken der Enigma wirklich kriegsentscheidend war, kann wohl nie genau beantwortet werden. Einschlägige militärhistorische Publikationen haben wahrscheinlich immer die Tendenz zu einer gewissen Einseitigkeit, je nach Standpunkt des Autors. Vielleicht kommt Georgi Shukow, ein Heerführer des Zweiten Weltkrieges, der Sache am nächsten, wenn er sagt: «Auch die gut funktionierende Aufklärung war ein Faktor in der Gesamtheit der Ursachen für den Erfolg».

2. Aufbau und Funktionsweise der Enigma

Wie bereits erwähnt, gibt es verschiedene Varianten der Enigma. Wir greifen hier diejenige heraus, die von der Schweizer Armee gebraucht wurde. Äusserlich besteht die Enigma aus einer Tastatur, zwei Lampenfeldern, vier Zahnrädern und einem äusseren Schlüsselfeld (Abb. 1). Die Zahnräder gehören je zu einer drehbaren Walze, welche aus einem Walzenkörper und einem relativ zum Walzenkörper drehbaren Walzenmantel besteht (Abb. 2). Der Walzenmantel ist aussen mit den 26 Buchstaben des Alphabets beschrieben, und zwar so, dass der Zentriwinkel zwischen zwei Buchstaben immer gleich (also = [360/26]°) ist. Die vier Walzen drehen alle um dieselbe Achse. Walze 4 (Umkehrwalze) ist fest, die anderen drei sind herausnehm- und untereinander permutierbar. Es gibt zwei Schlüssel, den inneren und den äusseren Schlüssel: Beim inneren Schlüssel wird auf jeder der vier Walzen der rote Pfeil auf dem Walzenkörper mit einem der 26 Buchstaben des Alphabets auf dem Walzenmantel in Übereinstimmung gebracht, dieser Buchstabe hat dann die Funktion des «Transportbuchstabens» für diese Walze (Abb. 3). Der äussere Schlüssel entsteht durch Drehung der 4 Zahnräder und somit der fest mit ihnen verbundenen Walzenmäntel: Er wird im äusseren Schlüsselfeld angezeigt und stellt den «Anfangszustand» der Walzen dar. Beim Chiffriervorgang wird der Klartext auf der Tastatur eingegeben und auf den beiden (identischen) Lampenfeldern wird das Chiffrat angezeigt (das zweite, durch Kabel mit der Maschine verbundene Lampenfeld dient zum Zwecke des «Zweipersonenbetriebs»: Eine Person gibt den Klartext ein, die zweite sitzt daneben und schreibt vom Lampenfeld das Chiffrat ab). Bei jedem eingetippten Buchstaben wird die Stellung der Walzen gemäss einem im folgenden beschriebenen Vorschubmechanismus verändert. Die Maschine ist so aufgebaut, dass, ohne einen Schalter zu betätigen, zum Dechiffrieren einfach wieder der Chiffretext eingetippt werden kann; hat man auf dem Lampenfeld auf diese Weise wieder den Klartext (man sagt deshalb, das Chiffrierverfahren der Enigma sei selbstinvers). Innerlich funktioniert die Maschine folgen-

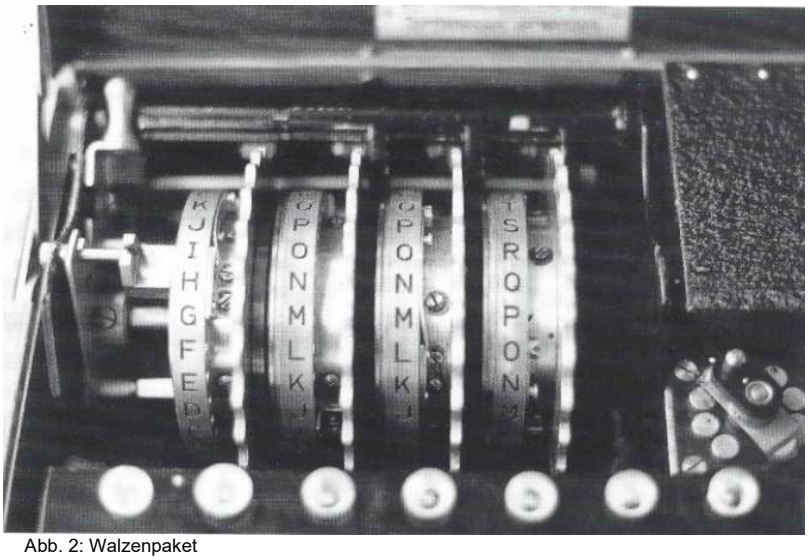

Abb. 2: Walzenpaket

dermassen: Jede der Walzen 1 bis 3 hat auf beiden Seiten je 26 kreisförmig gleichmässig auf dem Walzenkörper angeordnete Kontakte: rechts federnde Stifte und links Gleitkontakte; je ein Kontakt rechts ist mit je einem Kontakt links paarweise verbunden. Beim Stromdurchlauf durch Walze ***i*** ($1 \le i \le 3$) von rechts nach links erhält man also eine Permutation (d.h. umkehrbar eindeutige Abbildung des Alphabetes) Y_i, beim Stromdurchlauf von links nach rechts entsprechend die Umkehrpermutation Y_i^{-1}. Walze 1 (die Umkehrwalze) enthält nur auf der rechten Seite federnde Stiftkontakte, die innerhalb der Walze je paarweise verbunden sind. Diese Walze liefert also eine Permutation U des Alphabetes, welche selbstinvers (d.h. gleich ihrem Inversen) ist, für die also gilt

$U \bullet U^{-1} = E$

(wobei E die identische Permutation und die Nacheinanderausführung von Permutationen bedeuten). Nun läuft der Strom nach der Buchstabeneingabe zuerst durch die Walzen 1 bis 3, dann durch die Umkehrwalze, dann wieder zurück durch die Walzen 3 bis 1. Nach der Chiffrierung eines jeden Buchstabens erfahren die Walzen folgenden Vorschubmechanismus:

- Walze 1 wird immer um einen Buchstaben transportiert.
- Walze 2 wird genau dann um einen Buchstaben transportiert, wenn mindestens eine der folgenden zwei Bedingungen erfüllt ist:
  1. Der äussere Schlüsselbuchstabe der Walze 1 ist gleich dem inneren Schlüsselbuchstaben (d.h. Transportbuchstaben) von Walze 1.
  2. Der äussere Schlüsselbuchstabe der Walze 2 ist gleich dem inneren Schlüsselbuchstaben (d.h. Transportbuchstaben) von Walze 2.
- Walze 3 wird genau dann um einen Buchstaben transportiert, wenn der äussere Schlüsselbuchstaben von Walze 2 gleich dem inneren Schlüsselbuchstaben (d.h. Transportbuchstaben) von Walze 2 ist.
- Walze 4 (die Umkehrwalze) wird nicht transportiert.

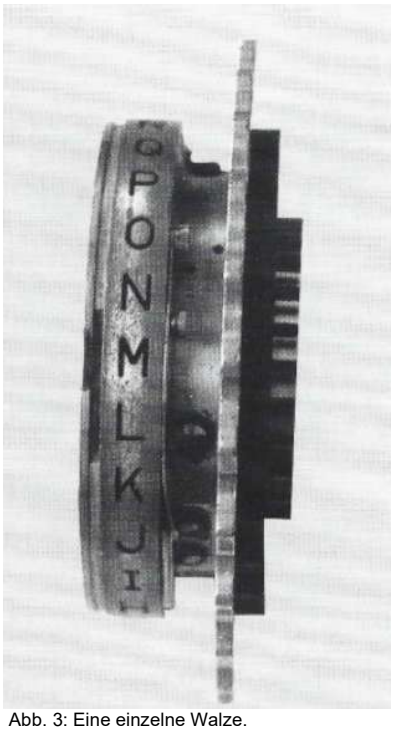

Abb. 3: Eine einzelne Walze.

Für das ganze Walzenpaket ergibt sich also (aufgrund der Permutierbarkeit der Walzen 1-3) eine Zahl von $6 \bullet 26^8 = 1.25 \bullet 10^{12}$ realisierbaren Permutationen (von insgesamt $26! = 26 \bullet 25 \bullet ... \bullet 1 = 4.03 \bullet 10^{26}$ total möglichen) des Alphabets. Die Anzahl möglicher Drehzustände des Walzenpakets beträgt 262-25= 16900.

Wir identifizieren im folgenden die 26 Buchstaben des Alphabets mit den Zahlen 1, 2.....26 und definieren Addition und Subtraktion wie bei Winkeln, wenn ein Vollkreis 26 Einheiten zählt (d.h. man addiert bzw. subtrahiert 26, wenn das Resultat ≤ 0 oder ≤ 27 ist, also z.B. 12 - 23 = 15 oder 23 + 12 = 9. Bezeichnen wir den äusseren Schlüssel mit (n_4, n_3, n_2, n_1), den inneren Schlüssel mit (m_4, m_3, m_2, m_1), den Winkel der Walze i gegenüber der Nullstellung (bei einem Vollkreis von 26 Einheiten) nach n chiffrierten Buchstaben mit $v_i(n)$, den n-ten Klartextbuchstaben mit K_n, den n-ten Chiffratbuchstaben mit Cn, die zyklische Permutation $1 \mapsto 2 \mapsto 3 \mapsto ... \mapsto 26 \mapsto 1$ mit Z, die k-fache Nacheinanderausführung von Z mit Z^k und die k-fache Nacheinanderausführung von Z^{-1} mit Z^{-k}, so erhalten wir

$v_i(0) = n_i - m_i \ (1 \le i \le 4)$ (1)

und

$C_n = A_n (K_n)$

$= (Z^{vi(n)} \bullet Y_1 \bullet Z^{-v1(n)+v2(n)} \bullet Z^{-v2(n)+v3(n)} \bullet Y_3 \bullet$

$\bullet (Z^{-v3(n)+v4(n)} \bullet U \bullet Z^{-v4(n)+v3(n)} \bullet Y_3^{-1} \bullet Z^{-v3(n)+v2(n)} \bullet$

$\bullet Y_2^{-1} \bullet Z^{-v2(n)+v1(n)} \bullet Y_1^{-1} Z^{-v1(n)}) \ (K_n)$ (2)

Da U selbstinvers ist, gilt dasselbe auch für A_n (denn $A = B \bullet U$, so ist

$A \bullet A^{-1} = B \bullet U (B \bullet U)^{-1} = B \bullet U \bullet U^{-1} \bullet B^{-1} = E.$)

3. Ansätze zur Dekryptierung der Enigma

Wir greifen zwei wichtige Dekryptierungsansätze heraus.

3.1 Dekryptierung bei bekannten Walzenschaltungen und bekanntem Klar- und Chiffrattext

Hier geht es also noch darum, den inneren und den äusseren Schlüssel zu bestimmen. Damit können dann alle weiteren Chiffrattexte, die mit demselben Schlüssel codiert worden sind, direkt dechiffriert werden.

Bezeichnet

$\overline{U}_n = Z^{v2(n)} \bullet Y_2 \bullet Z^{-v2(n)+v3(n)} \bullet Y_3 \bullet Z^{-v3(n)+v4(n)} \bullet U \bullet$

$\bullet Z^{-v4(n)+v3(n)} \bullet Y_3^{-1} \bullet Z^{-v3(n)+v2(n)} \bullet Y_2^{-1} \bullet Z^{-v2(n)}$

die Permutation, die «links von Walze 1» bei der Chiffrierung des n-ten Buchstabens aus-

geführt wird (also nur durch den Stromdurch- und -rückfluss durch die Walzen 2 → 3 → 4 → 3 → 2), so ist ebenfalls $\overline{U}_n$ selbstinvers und es folgt

$A_n = Z^{-v1(n)} \cdot Y_1 \cdot Z^{-v1(n)} \cdot \overline{Un} \cdot Z^{v1(n)} \cdot Y_1^{-1} \cdot Z^{-v1(n)}$ (3)

Setzt man $\Psi = n_1 - m_1$, so gilt (da Walze 1 bei jedem Schritt um einen Buchstaben weitergeführt wird), $v_1(n) = \Psi + n$. Setzt man dies in (3) ein, ergibt sich

$A_n = Z^{\Psi+n} \cdot Y_1 \cdot Z^{-\Psi-n} \cdot \overline{U}_n \cdot Z^{\Psi+n} \cdot Y_1^{-1} \cdot Z^{-\Psi-n}$ (4)

oder, aufgelöst nach

$\overline{U}_n = Z^{\Psi+n} \cdot Y_1^{-1} \cdot Z^{-\Psi-n} \cdot A_n \cdot Z^{\Psi+n} \cdot Y_1 \cdot Z^{-\Psi-n}$. (5)

Jeweils nach dem Transport der Walze 2 bleiben die Grössen $v_2(n)$, $v_3(n)$, $v_4(n)$ und somit während mindestens 25 Schritten konstant (25 Schritte, wenn Walze 3 mitgedreht wird, sonst 26). Das hat aber zur Folge, dass es innerhalb eines jeden Intervalls von 26 aufeinanderfolgenden Buchstaben im Klartext irgendwo ein mindestens 12-buchstabiges Teilintervall geben muss, auf dem die Permutation $\overline{U} \equiv \overline{U}_n$ unverändert bleibt. Für jedes mögliche $\Psi \in \{0, 1, \ldots, 25\}$ untersucht man nun die Permutation

$(C_{j+1}, C_{j+2}, \ldots, C_{j+12}) = (\overline{U}(K_{j+1}), \overline{U}(K_{j+2}), \ldots, \overline{U}(K_{j+12})$ (6)

($\overline{Un}$ wie in (5)) auf Selbstinversheit. (Selbstinversheit kann sehr einfach geprüft werden: Findet man $a \mapsto b$, so muss einfach auch die Umkehrrelation $b \mapsto a$ gelten (für alle a, b).) Bleibt nicht bereits jetzt ein widerspruchsfreies Ψ über, so fährt man mit der Buchstabenfolge (C27, C28, ..., C38) weiter, usw. (d.h. man rutscht immer um 26 Buchstaben). Im Idealfall bleibt am Schluss ein einziges widerspruchsfreies Ψ und damit eine eindeutige Funktion $n \mapsto v_1(n) = \Psi + n$ übrig. Die Bestimmung der Funktionen $n \mapsto v_1(n)$ ($2 \le i \le 4$) geschieht analog.

3.2. Dekryptierung bei bekannter Walze 1 und einem «mot probable»

Es ist ein allgemeines Phänomen in der Kryptologie, dass sog. «mots probables» (d.h. Wörter, die man im Klartext vermutet) das Dekryptieren wesentlich vereinfachen können. Deshalb sollte z.B. im militärischen Bereich vorsichtig umgegangen werden mit oft auftretenden Wörtern wie etwa «Division», «Flugzeug», «Gegner», usw. Wie oben erwähnt, waren die Deutschen im Zweiten Weltkrieg sehr unvorsichtig mit solchen «mots probables». Die Methode mit einem «mot probable» kann im Prinzip auf das soeben erklärte Verfahren zurückgeführt werden, wenn man einfach das «mot probable» mit beliebigen Sequenzen aufeinanderfolgender Buchstaben der entsprechenden Länge im Chiffrattext in Beziehung setzt. Dabei zeigt es sich, dass oft schon die Kenntnis von Walze 1 reicht, um nur eine widerspruchsfreie selbstinverse Permutation zu erhalten.

4. Zusammenfassung und Ausblick

Die Selbstinversheit vereinfacht zwar die Handhabung der Enigma ganz beträchtlich, da man, ohne die Maschine umzuschalten, chiffrieren und dechiffrieren kann. Andererseits ist dies auch eine Schwäche; man beachte, dass der oben erwähnte Dekryptieransatz gerade auch auf dieser Selbstinversheit beruht.

Die Kryptologie hat in den letzten 20 Jahren weltweit einen riesigen Aufschwung genommen, und zwar einerseits durch sehr tiefliegende theoretische Arbeiten und andererseits durch die Verfügbarkeit immer leistungsfähigerer Hardware, die selbst wiederum das Bedürfnis nach einem vernünftigen Datenschutz hervorgerufen hat (Stichworte wie Mobiltelefone, Datenbanken, elektronischer Zahlungsverkehr, Internet, usw. mögen dies belegen). Ein Meilenstein war das 1977 von R. Rivest, A. Shamir und L. Adleman publizierte sog. RSA-Verfahren mit öffentlichem Schlüssel. Das Verfahren beruht auf nichts anderem als einerseits einem einfachen Satz aus der Algebra (dem sog. «Kleinen Satz von Fermat» [1601-1655]) und andererseits auf der Tatsache, dass es bis jetzt keinen «schnellen» Algorithmus zur Primfaktorzerlegung zu geben scheint (eine strenge Herleitung dieser letzten Aussage wäre möglich nach der Lösung sehr schwieriger, heute noch offener Probleme der analytischen Zahlentheorie). Der Kleine Satz von Fermat besagt, dass für jede endliche Gruppe $\boldsymbol{G}$ der Ordnung n mit neutralem Element e und jedes Element $g \in \boldsymbol{G}$ gilt $g^n = e$. Er ist nicht zu verwechseln mit dem sog. «Grossen Satz von Fermat» über die Nichtlösbarkeit der Diophantische Gleichung $x^n + y^n = z^n$ für $n \ge 3$, welcher erst kürzlich bewiesen werden konnte mit Hilfe von Theorien, die ihrerseits wiederum unter anderem die Monte-Carlo-Simulationstechnik weitergebracht haben. Wie würde wohl die Landkarte heute aussehen, wenn bereits vor dem Zweiten Weltkrieg jemand die Verwendbarkeit des 300 Jahre alten Kleinen Fermatschen Satzes zur effizienten Datenverschlüsselung geahnt hätte...?

Literatur

Bauer, F.L. (1995). *Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie.* Springer, Berlin.

Konheim, A.G. (1981). *Cryptography. A Primer*. Wiley, New York.

Kozaczuk, W. (1987*). Im Banne der Enigma. Ereignisse, Tatsachen, Zusammenhänge.* Militärverlag der Deutschen Demokratischen Republik VEB, Berlin. Schweizerische Armee (1981). KryptologenHandbuch.

Sieber, E., Haeberli, W., Gruner, E. (1979). *Weltgeschichte des 20. Jahrhunderts*. Eugen Rentsch, Erlenbach-Zürich.