Luxemburger Wort
Donnerstag, den 7. Juni 2012 ❖ Nummer 18|2368

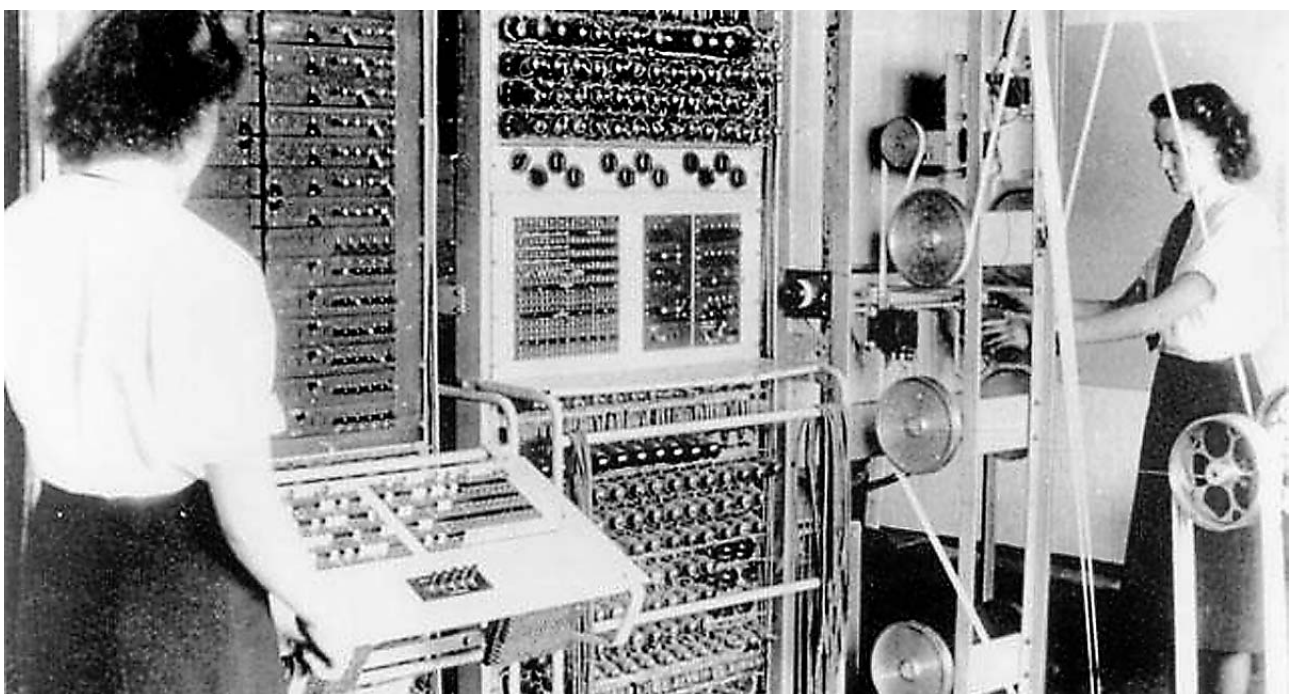
Sie veränderte den Lauf der Geschichte

Eine geheime unbekannte Maschine

Kryptologie als Geheimwaffe im Zweiten Weltkrieg

André Schwarz

Am 1. Juni 1944 nehmen britische Ingenieure eine völlig neuartige „Maschine“ in Betrieb. Eine „Maschine“ die unbedingt notwendig ist, damit die anstehende Landung in der Normandie überhaupt Aussicht auf Erfolg haben kann. Denn die Alliierten sind sich längst bewusst, dass sie dazu über wesentlich mehr strategisch zuverlässige Informationen verfügen müssen, als ihnen Luftaufklärung, Überläufer, Agentennetze oder Spione liefern können.



Tommy Flowers' neuartige „Maschine“ namens COLOSSUS ist der weltweit erste vollelektronische digitale Computer und lieferte den Alliierten genaue und zuverlässige Informationen für die Landung in der Normandie.
(Foto: Bletchey Park Museum)

Der Funkverkehr des Gegners enthält alle benötigten Informationen über Stationierungen, geplante Verlegungen, Operationen oder Kampfstärke der Truppen und bietet sich als „die“ Quelle an. Und diese neuartige „Maschine“ soll es den Alliierten erlauben, all diese Informationen, obwohl verschlüsselt übertragen, zeitnah mitzulesen. Eine „Maschine“ deren bloße Existenz alle Beteiligten während der folgenden 40 Jahren leugnen müssen.

Neuer Moment in der Kryptologie

Verschlüsselungen von Botschaften sind bereits seit Julius Cäsar üblich, wie auch regelmäßige Entschlüsselungen. Im Jahre 1926 tritt jedoch ein neuer Moment auf. Polen, das sich der latenten Kriegsgefahr bewusst ist, scheitert trotz seiner Erfahrungen daran, die Funksprüche der deutschen Marine und des Heeres mit den bekannten kryptanalytischen Methoden zu dechiffrieren. Bald bestätigt sich der Verdacht, dass die Deutschen eine neuartige maschinelle Chiffrierung anwenden, die nur durch wissenschaftliche Methoden zu brechen ist. Mit vom französischen Geheimdienst beschafften Unterlagen und mit viel intuitiver Logik gelingt den Polen die Brechung der ENIGMA I-Verschlüsselung. Es ist der erste Beweis dafür, dass zur erfolgreichen Kryptanalyse maschineller Chiffrierungen „intelligence“ erforderlich ist: Diese beschafft man durch Diebstahl oder Kopie und durch Kompromittierung: Der polnische Mathematiker Rejewski beobachtet Häufungen bestimmter Schlüssel durch schlechte Gewohnheiten der Operatoren und konstruktionsbedingte Unzulänglichkeiten und wertet diese mit der mathematischen Gruppentheorie aus.

Ab September 1938 macht ein Verfahrenswechsel die Dechiffrierungen unmöglich. Doch Zygalski kann mit seinem Lochkartenverfahren („Zygalski Sheets“) schon bald wieder dechiffrieren und ab November stehen dafür sechs schnelle elektromechanische BOMBA-Maschinen zur Verfügung, die Palluth mittels eines von Rejewski erarbeiteten Algorithmus entwickelt hat. Im Januar 1939 erfolgen weitere Modifikationen der ENIGMA. Die damit erforderliche Aufstockung an BOMBA-Maschinen und Fachpersonal überfordern schlicht die Ressourcen des polnischen Geheimdienstes.

Station X übernimmt

In den 30er-Jahren gelingt es Alfred D. Knox, in den Diensten der britischen Geheimdienstes MI6 stehend, mittels linguistischer Kryptanalyse die im spanischen Bürgerkrieg verwendete ENIGMA D zu entziffern. Doch bei der ENIGMA I muss er passen, da Knox, obwohl ein erfahrener Linguist, Probleme bei der Entzifferung der zu komplexen Chiffrierungen hat. Erst als bei einem Treffen im Juli 1939 aufgrund der offenkundigen Kriegsgefahr die Polen den verblüfften Experten Englands und Frankreichs die Funktion ihrer BOMBA und des Lochkartenverfahrens erklären und ihnen dabei auch ihre Unterlagen, Lochkarten und nachgebaute ENIGMA I übergeben, besteht die Hoffnung, möglichst bald wieder die deutschen Funksprüche mitlesen zu können.

Die Unterzeichnung des Molotow-Ribbentrop-Paktes am 23. August 1939 und damit die Gewissheit, dass der Krieg unausweichlich ist, veranlasst die Kryptanalytiker des MI6, ihre Arbeitsstätte in das abgelegene Bletchley Park

Mit COLOSSUS ermöglichte der britische Elektroingenieur Tommy Flowers den Alliierten, die strategisch wichtigen Geheimnachrichten zwischen Hitler und seinen Generälen mitzulesen.
(Foto: webfronter.com)

(BP) 40 Meilen nördlich von London zu verlegen, um hier unter dem Decknamen Station X bis Ende 1945 zu arbeiten. Bereits in den Monaten vor Kriegsausbruch sucht Alastair Denniston die britischen Universitäten ab nach geeigneten Mathematikern und Linguisten, die als Codebrecher eingesetzt werden können. Um die neuen Mitarbeiter in BP unterbringen zu können, verlegt man die Arbeitsplätze in vorgefertigte Holzhütten, die berühmten „huts“. Aus Geheimhaltungsgründen werden die verschiedenen Sektionen in BP nur noch mit ihrem „hut“-Namen geführt. Den Verantwortlichen wird auch klar, dass die zu erwartende Unmenge an militärischen Informationen die Kapazitäten von Knox' bisheriger Sektion sprengen werden. Daher muss zusätzlich zu der Dechiffrierung eine eigenständige Auswertungssektion kommen und auch der Kontakt zu den Funk-Abhörstationen, den so genannten „Y-Services“, muss wesentlich verbessert werden. Damit entsteht in BP die weltweit erste „Produktionslinie zur militärischen Informationsgewinnung“.

Turings BOMBEn

Bereits als visiting fellow in Princeton baut der Mathematiker Alan Turing[1] 1937 seine erste kryptologische Maschine. Ende 1938 belegt er Kryptologie-Kurse des MI6 und assistiert Knox bei dessen ersten Versuchen, die Enigma I zu attackieren. Im September 1939 verpflichtet man ihn als hauptberuflichen BP-Mitarbeiter und erteilt ihm den Auftrag, nach Methoden zu suchen, die die Schwächen des polnischen Entzifferungsverfahrens vermeiden. Turing findet eine Lösung: Er ersetzt in verschlüsselten Funksprüchen den fehlenden Klartext durch die Annahme eines Wortes, das im Text wahrscheinlich vorkommt (probable word) und dessen Stellung ungefähr bekannt ist. Beispielsweise senden deutsche Dienststellen täglich einen verschlüsselten Wetterbericht, in denen fast sicher das Wort „Wetter“ enthalten ist und den strengen deutschen Vorschriften nach muss sich dieses an einer bestimmten Position befinden. Diese Klartextfragmente nennt man „crib“, und Turing geht davon aus, dass mit Hilfe dieser „cribs“ der jeweilige ENIGMA-Schüssel rekonstruierbar ist. So schafft er es im Dezember 1939, ENIGMA-Funksprüche aus dem Jahre 1938 zu entziffern, aber keine aktuellen Funksprüche. Um herauszufinden, warum dies ihm nicht gelingt, trifft er im Januar 1940 in der Nähe von Paris die inzwischen geflüchteten Polen. Mit den von den Briten wesentlich erweiterten „Zygalski Sheets“ gelingt es ihnen zum ersten Mal, in den ENIGMA-Kriegsverkehr einzubrechen.

Um die Dechiffrierung wesentlich zu beschleunigen, entwirft Turing eine elektromechanische Machine, die im März 1940 in Betrieb geht. „Victory“ enthält 30 rotierende Trommeln und simuliert somit gleichzeitig die Aktion der Räder von zehn ENIGMA-Maschinen. Damit können alle verschiedenen Möglichkeiten der Schlüsselräder-Einstellungen durchprobiert werden, um zu sehen, ob der vermutete Klartext im abgefangenen Funkspruch erscheint. Jedes Mal, wenn Turings BOMBE eine mögliche Übereinstimmung findet, wird diese auf einer kryptologisch verbesserten ENIGMA (TYPEX) ausprobiert, um zu sehen, ob ein deutschsprachiger Text erscheint. Wenn dies der Fall ist, wird dieser zur Informationsgewinnung an „hut 3“ weitergeleitet. Im August 1940 geht eine zweite nach einer Idee von Gordon Welchman modifizierte BOMBE („Agnus Dei“) in Betrieb, wobei er seine Theorie, dass die ENIGMA-Verschlüsselungen umkehrbar sind, umsetzt[2]. Dadurch, dass nun diese beiden Möglichkeiten gleichzeitig getestet werden, steigt die Effizienz der Suche drastisch an, und man kommt zudem mit kürzeren „cribs“ aus. ▶

▶ ULTRA

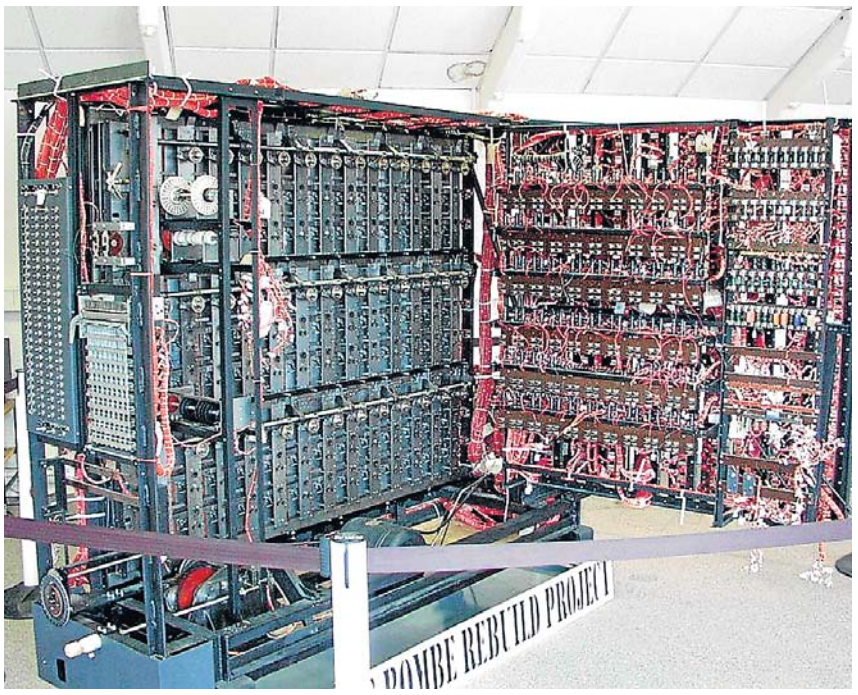
Wie bereits erwähnt, braucht man neben Maschinen auch „intelligence“. Und diese besorgen sich die Briten, indem sie z.B. deutsche Wetterschiffe, Frachter oder U-Boote kapern. Mit deren Codebüchern, mit immer häufigeren „cribs“, einer wachsenden Anzahl von BOMBEN und dem von Turing erfundenen „Banburismus“-Verfahren gelingt es Turings Team, die deutsche Marine-ENIGMAs „Dolphin“ und „Shark“ mit Unterbrechungen bis zum Kriegende mitzulesen und so alliierte Schiffskonvois vor den lauernden deutschen U-Booten zu retten. Andererseits bleibt die unter dem Codenamen „Red“ geführte Luftwaffen-ENIGMA wegen ihrer mangelhaften Verschlüsselung bis zum Kriegsende eine sprudelnde „intelligence“-Quelle, da sie wegen ihrer Heeresunterstützung indirekt über dieses Informationen liefert.

Darüber hinaus veranlassen die Entzifferer in BP deutsche Dienststellen bekannte Begriffe unfreiwillig zu verschlüsseln („gardening“): Sie lassen beispielsweise eine Markierungstonne einer Hafeneinfahrt zerstören, und können dann sicher sein, sehr bald chiffrierte Warnmeldungen zu erhalten wie „Markierungstonne Einfahrt Calais zerstört“ usw. Überdies verbreiten die deutschen Dienststellen diese Warnmeldungen fast immer mit verschiedenen Verfahren verschlüsselt, dazu wortgleich, womit BP dann per Klartext-Geheimtext-Kompromittierungen ungelöste Probleme mit Verschlüsselungen lösen kann.

Diese hervorragenden wissenschaftlich-technischen Leistungen erbringen die etwa 10 000 Mitarbeiter in BP, das damit zum weltweiten Zentrum der maschinellen Kryptanalyse wird. Ihr Material erhalten sie von den Abhör- und Peilstationen, die der „Y-Service“ weltweit errichtet hat. Der Personalbedarf dafür ist immens, so arbeiten z.B. nur in einer Station [Beaumanor (GB)] 1 200 Personen in vier Schichten. Dieser Aufwand ist erforderlich für das Abhören aller Frequenzen, Überwachung deren Funkaktivitäten und die korrekte Aufzeichnung der Sendungen. Die Mitarbeiter in BP und des Y-Service bilden die bis 1974 geheimgehaltene Organisation ULTRA. Diese entziffert fast alle erreichbaren Funksendungen nicht nur der deutschen Wehrmacht, sondern auch der Abwehr, der Reichsbahn, der SS, der Polizei usw. Dazu kommen italienische Militärsendungen, die für den Mittelmeer-Krieg sehr wichtig sind, und die häufigen, meist sehr informativen Sendungen der japanischen Botschaft in Berlin.

Einer der gröbsten Chiffrierfehler geschieht, als Karl Dönitz am 30. Januar 1943 seine Beförderung zum Großadmiral und Oberbefehlshaber allen Marinedienststellen und durch Funk den Schiffen mitteilen lässt. Die zuständigen Nachrichtenoffiziere (wegen fehlender elementarer kryptologischer Kenntnisse) lassen den Text *wortgleich* mit *allen* relevanten Verfahren verschlüsseln und dann senden, und liefern so den Kryptologen in BP für alle Marine-Chiffrierverfahren eine Klartext-Geheimtext-Kompromittierung, ein Super-„depth“. Überdies war die Verschlüsselung unsinnig, denn es ist keine Geheimnachricht – sie steht am nächsten Tag in den Zeitungen.

Die Sammlung und Auswertung aller Informationen verschafft eine einmalige informelle Überlegenheit (was der geniale Stratege Winston Churchill im Gegensatz zu den Deutschen früh-



Wie überragend die Leistungen des Ingenieurs Harold Keen und dessen Team bei Konstruktion und Bau waren, offenbarte sich erst, seitdem rezent versucht wird, in BP eine solche BOMBE zu rekonstruieren.

(Foto: Tom Yates über wikipedia.de)

zeitig erkannt hat): Neben taktischen Informationen für den U-Boot-Krieg, ermöglicht sie z.B. den Alliierten vor kritischen militärischen Ereignissen das Führungsverhalten der dabei kommandierenden deutschen Offiziere meist richtig zu prognostizieren, weil deren Persönlichkeitsprofile im Laufe des Krieges erarbeitet worden sind.

Man geht keine Risiken während des Kriegs in England ein: Der umfangreiche (bis eine Mio. Worte pro Tag) und militärisch wichtige Nachrichtenaustausch per Fernschreiber mit den USA ist wegen der großen Länge der Texte durch Kryptanalyse besonders gefährdet. Um diesen Nachrichtenverkehr zu sichern, entwickelt der MI6 eine besonders sichere Version des One Time Pad-Verfahrens, genannt ROCKEX. Dessen nur einmal verwendete Schlüssel erzeugt man nicht maschinell, sondern tastet elektronisches Rauschen ab. Darüber hinaus verschleiert man elektronisch die Betriebszeichen (Zeilenvorschub usw.), um jegliche Möglichkeit der Schlüsselanalyse auszuschließen.

TUNNY gegen SZ42

Nachrichten mittels ENIGMA zu verschlüsseln, ist langsam und benötigt mehrere Operateure. Jeder Buchstabe wird einzeln eingegeben, und das aufleuchtende Zeichen wird per Hand notiert und anschließend wird der ganze Text mit zusätzlichen Kennzeichen per Morse-Code gesendet. Wesentlich schneller sind die Geheimfernschreiber Lorenz SZ („Tunny“) und Siemens und Halske T52 („Sturgeon“), doch ihre Dechiffrierung ungleich schwieriger. Bereits 1940 gelingt es den Schweden, die T52a/b zu brechen. Den Briten verhelfen die deutschen Operatoren mit ihrem „operator chat“ in Klartext und einem unsachgemäßen Gebrauch zu genügenden „depths“, um auch die T52c zu entziffern. London interessiert sich vor allem für die vom Heer betriebenen SZ42-Linien: Über diese läuft die Kommunikation der obersten deutschen Führungsebene (Hitler, OKW, Heeresgruppen), eine Entzifferung der Kommunikation würde den Alliierten kaum abschätzbare Vorteile für ihre strategischen Planungen bringen.

Im August 1941 geschieht ein schwerwiegender Fehler bei Testsendungen, der es den BP-Kryptologen Tiltmann und Tutte der „Tunny“-Abteilung ermöglicht, bis Januar 1942 den Algorithmus der Chiffrierung zu erarbeiten. Um diesen maschinell auszuwerten, konstruiert die Britische Post in ihrem Forschungslaboratorium in Dollis Hill einen SZ42-Simulator aus Telefon-Hubdrehwählern und Relais („Tunny machine“). Doch zur Entzifferung braucht man zusätzlich auch die SZ42-Schlüsselräder, die sich nur mit großem personellen Aufwand kryptanalytisch ermitteln lassen. Zu einer prekären Lage kommt es im August 1942, als, bedingt durch ein neues von der Wehrmacht eingesetztes Verfahren, sich diese nicht mehr ermitteln lassen. Man muss auf Turing zurückgreifen, der eine neue (nicht maschinelle) Entzifferungsmethode namens „Delta-K“ entwickelt, auch „Turingery“ genannt, die durch Tutte zur „statistical method“ erweitert wird.

Damit gelingt es im Januar 1943, die neue SZ42-Fernschreiblinie zwischen Rom und Rommels Hauptquartier in Tunesien mitzulesen, und BP kann mit diesen Informationen die Entscheidungskämpfe an der Afrikafront beeinflussen. Allerdings erfordert das einen enormen personellen Aufwand, da damals nur Tabelliermaschinen als Hilfsmittel zur Verfügung stehen, um die Tagesschlüssel der SZ42-Maschine zu bestimmen.

Der Mathematiker und Leiter der Tunny-Abteilung Max Newman schlägt vor, diese umfangreichen Zählprozesse durch elektronische Zählschaltungen zu beschleunigen. Bereits im Juni 1943 arbeitet die „HEATH ROBINSON“, die gleichzeitig zwei Lochbänder photoelektrisch mit je ca. 1 000 Zeichen/sek. liest, eines mit der Schlüsselsequenz, das andere mit dem Geheimtext, und beide als Endlosschleife verklebt. Der Leseprozess startet mit einem Versatz um ein Zeichen, so dass nach jedem Umlauf eine andere Phasenlage entsteht.

Die gelesenen Impulsfolgen steuern die „combining unit“ (von Tommy Flowers entworfen), die die beiden Impulsströme per Boolescher Algebra vergleicht. Die resultierenden Übereinstimmungen zählt dann die von Wynn-Williams konstruierte teil-elektronische digitale Zählschaltung. Besondere Probleme bereiten häufige Bandrisse wegen der erforderlichen vielen schnellen Umläufe. Überdies bringen Synchronisationsprobleme infolge Lochbanddehnungen den kryptanalytischen Prozess außer Tritt. Auch die nachfolgende SUPER-ROBINSON scheitert an diesen Problemen.

COLOSSUS I und II

Flowers schlägt stattdessen eine komplett neue Maschine vor, vollelektronisch digital arbeitend und nur mit einem Band zur Eingabe, um Synchronisationsfehler von vorneherein auszuschließen. Für die Realisierung rechnet er mit ca. 2 000 Röhren für die gesamte Elektronik, doch das gilt in BP wegen der zu erwartenden Unzuverlässigkeit als nicht akzeptabel: Schon der Ausfall einer einzelnen Röhre könnte zu großen Rechenfehlern führen, und überdies würde man das bei digitalen Logikschaltungen kaum sofort bemerken, so der damalige Wissensstand. Der einzige, der das Projekt nicht ablehnt ist Newman, er lässt sich von Flowers' Vorkriegs-Erfahrungen mit Röhren bei Telefonzentralen überzeugen.

Der kriegsbedingte Zeit- und Erfolgsdruck zwingt Flowers, sofort mit der Konstruktion zu beginnen; Zeit für Testschaltungen, um seine Ideen zu prüfen, bleibt nicht. Er ersetzt die Synchronisierung durch eine Taktsteuerung, damals eine völlig neue Idee. Dazu wird das Geheimtextband mit 5 000 Ziffern/sek. fotoelektrisch gelesen, und dessen Transportlochung steuert als Taktgeber das gesamte System. Den Speicher für die fünf Kanäle des Fernschreib-Codes entwirft er als fünffaches Schieberegister mit Thyratronröhren, das den Schlüsselstrom entsprechend dem SZ42-Algorithmus erzeugt. Diese Bit-Folge vergleicht die Maschine (alle fünf Kanäle parallel!) per Boolescher Logik mit dem eingelesenen Geheimtext mittels von Newman und Tutte entworfenen kryptanalytischen Algorithmen. Dabei gefundene Übereinstimmungen werden gezählt und die Ergebnisse zwischengespeichert.

Den störungsfreien Betrieb mit 1 500 Röhren (später 2 500 bei COLOSSUS II) gewährleistet er (was damals als nicht realisierbar gilt), durch Herabsetzen der Röhrenleistung auf 30 % und Dauerbetrieb bei konstanten Temperaturverhältnissen. Nach nur neun Monaten Planungs-, Bau- und Montagezeit kann der neuartige Rechner in Betrieb genommen werden, wobei Leistung und Betriebssicherheit die Erwartungen übertreffen. ▶

[1] Ein Unbekannter, Unsterblicher, in DIE WARTE vom 7. Juni 2007

[2] Welchmans Annahme war richtig. Die ENIGMA-Konstrukteure Schrebius und Korn glaubten, wie die interessierten Militärs, dass durch einen zweimaligen Stromdurchgang durch die Walzen die Chiffrierung verstärkt würde. Aber damit erreichten sie das Gegenteil: Die Maschine wurde reziprok, d.h. Chiffrierung und Dechiffrierung erfolgten bei gleicher Einstellung, und erleichterte den Kryptanalytikern die Arbeit sehr. Es ist ein Musterbeispiel dafür, wenn kryptologische Laien auf empirischer Basis eine elektromechanisch hervorragende Maschine entwickeln und bauen und glauben (wie ihre Abnehmer wohl ebenso), dass die theoretisch ermittelte große Zahl der Schlüsseleinstellungen der ENIGMA allein deren Sicherheit ausmachen würde.

Luxemburger Wort
Donnerstag, den 7. Juni 2012 ❖ Nummer 18|2368

Wer ist gemeint?

Das Bauen der Renaissance prägte er wesentlich mit

Wer auch nur halbwegs mit der Stadt Rom vertraut ist, weiß um die Sehenswürdigkeiten, die das Quartier rund um die Piazza Santa Maria in Trastevere bereithält. Nur wenige Gehminuten von der Porta Aurelia entfernt trifft man beispielsweise auf ein steinernes Meisterwerk der Hochrenaissance, nämlich eine kreisrunde, mit Säulen und Kuppel versehene Kapelle. Nach den Vorstellungen des Architekten hätte die angrenzende Bebauung auf die dadurch vorgegebenen Proportionen ausgerichtet werden sollen. Dazu kam es aber nicht. Also sehen wir das stilbildende „Tempietto“ im Innenhof eines Klosters.

Der heute Gesuchte lieferte Konstruktionspläne für etliche Sakralbauten. Sein berühmtestes und zweifellos folgenreichstes Projekt konnte er allerdings nur in der Anfangsphase leiten; danach wurden Michelangelo, Carlo Maderno, Gian Lorenzo Bernini und viele andere daran beteiligt. Im Verlauf der bis ins 17. Jahrhundert andauernden Bauarbeiten nahm diese Kirche denn auch eine völlig andere Gestalt an, als es vom ersten Auftragnehmer beabsichtigt worden war – lediglich ein Treppenturm entging dem umgestaltungsfreudigen Zugriff seiner Nachfolger.

Über Kindheit und Jugend des hier zu Enträtselnden liegen wenige gesicherte Informationen vor. Nicht einmal der Tag seiner Geburt ist überliefert. Mit der Aufnahme beruflicher Tätigkeit gewinnt diese Biografie jedoch zügig an Kontur. So ist ein Wirken in Bergamo und Vigevano nachweisbar; als wichtiger Aufenthaltsort wird Mailand genannt. Seine Übersiedlung an den Tiber lässt sich einem militärisch bedingten Wechsel der lokalen Machtverhältnisse zuschreiben.

70 Jahre soll das Leben dieses Mannes gewährt haben. An dem, was er ins Werk gesetzt hatte, orientierten sich noch zahlreiche Kreative. Zugleich gab es immer wieder Klagen, weil auch überaus Erhaltenwertes abgerissen worden war. Das ihm in seiner Zeit angehängte Etikett „Maestro Ruinante“ ist unvergessen. Enzyklopädien verzeichnen den nun in groben Zügen Dargestellten unter einem Beinamen, der von seinem Großvater mütterlicherseits stammt. – Um wen handelt es sich?

Christian Schnitzler

Auflösung:

Diese Zeilen gelten Donato di Angelo di Antonio, der in den Quellen auch als di Pascuccio d'Antonio auftaucht und gemeinhin Bramante genannt wird. Er kam um 1444 in Monte Adrualdo nahe Fermignano zur Welt und starb am 11. März 1514 in Rom. Papst Julius II. beauftragte ihn mit dem Neubau des Petersdoms.

Eine geheime unbekannte Maschine

▶ In COLOSSUS II, am 1. Juni 1944 betriebsbereit, können zusätzlich bedingte Sprungbefehle und Verzweigungen geschaltet werden, weil Verbesserungen der SZ42 (und die geplante Landung) dies erfordern. Mit den nach und nach installierten zehn COLOSSI II kann BP die Schlüsselstellungen (wheel settings) meist innerhalb weniger Stunden ermitteln. Damit kann anschließend die „Tunny machine“ den Klartext erzeugen – überwiegend längere Texte der obersten Führungsebene der Wehrmacht.

US-Technik: Desch-US-BOMBE und Mark I

Bereits im Dezember 1940 besucht eine US-Delegation inoffiziell BP und wird dort umfassend informiert. Im Oktober 1942 treffen sich Travis (BP) und Wenger (US-Navy) und vereinbaren ihre Zusammenarbeit bei der Brechung deutscher Marine-Chiffrierungen. Denn nach Einführung der komplexeren Marine ENIGMA M4 gelingt es den Briten nicht rechtzeitig, genügend leistungsfähige BOMBE-Maschinen zu bauen. Die US-Navy beschließt, schnelle vollelektronische Vier-Rotoren-Maschinen zu entwickeln. Der damit beauftragte Joseph Desch von der Firma NCR hält dafür ca. 20 000 Röhren für erforderlich (was damals als unmöglich zu betreiben gilt) und beschränkt sich daher (mit Turings Unterstützung), die britische Rotoren-Mechanik mit schnellen elektronischen Zählern und Vergleichern zu kombinieren. Die zur Entzifferung unentbehrlichen „cribs“ liefert im Übrigen BP über eine sichere Fernschreiber-Übertragung. Der BRUSA-Pakt vom Mai 1943 gewährt US-Experten überall Zutritt in BP und ermöglicht eine intensive und erfolgreiche Zusammenarbeit ohne Geheimnisse voreinander. In der Spätphase des Krieges machen fehlende „cribs“ die BOMBE-Maschinen unbrauchbar; das Problem löst eine neue US-Maschine (FILBUSTER), deren Aufbau und Funktion bis heute geheim gehalten wird. In Harvard betreibt Howard Aiken[3] seinen von ihm entwickelten und von IBM gebauten vollautomatischen elektromechanischen Rechner Mark I, der aber vor allem zu ballistischen Berechnungen und zur Lösung von Differentialgleichungen für das Manhattan-Projekt verwendet wird, jedenfalls nicht für kryptanalytische Berechnungen.

ENIAC versus COLOSSUS

Im Vergleich zu COLOSSUS muss man ENIAC bei seiner Inbetriebnahme 1945/46 als technisch veraltetes System bezeichnen. Dies wird verständlich, wenn man den historischen Hintergrund einbezieht: Die US-Artillerie benötigt ballistische Tabellen, die sie seit 1934 mit Hilfe des mechanisch-analogen „Bush-differential analyzer“ berechnen lässt. Mit Kriegsbeginn braucht die Army dringend ein schnelleres und genaueres System. Im Juni 1943 beginnt daher in der Moore School of Electrical Engineering ein Team unter Eckert und Mauchly mit der Entwicklung des ENIAC. Heraus kommt eine leistungsstärkere elektronische Version des „differential analyzer“, ein „number cruncher“, den nach Kriegsende eigentlich niemand mehr benötigt. Es scheint auch heute eindeutig zu sein, dass man sich Tommy Flowers' Erkenntnisse, die er bereits 1943 über den Dauerbetrieb von Elektronenröhren bei COLOSSUS gewonnen hatte und die auch den US-Experten in BP bekannt waren, bei der Konstruktion bedient hat. Weiterhin sind es interessanterweise gerade die detaillierten Aufzeichnungen der US-Experten von 1943 über COLOSSUS die das COLOSSUS-Rebuild-Project im BP-Museums realisierbar machen. Auch wenn COLOSSUS zu kryptanalytischen Zwecken entwickelt wurde, so entspricht sein Konzept der Turingschen Idee und damit bereits den uns heute geläufigen Computern[4].

Winston Churchill erkannte schon in den 20er-Jahren die militärische Informationsgewinnung mittels Kryptoanalyse als strategischen Vorteil und ermöglichte, dass Bletchey Park zum weltweiten Zentrum der maschinellen Kryptanalyse wurde.

Als jedenfalls 1996 das 50. Jubiläum des ENIAC in den USA mit den Begriffen „the world's first large-scale electronic digital computer“ und „birth of information age“ gefeiert wurde, war dies zwar verständlich, aber komplett falsch. Verständlich daher da wegen Geheimhaltungsgründen die Briten bis 1974 sogar die bloße Existenz von COLOSSUS und ULTRA leugneten. Erst 2000 wird der „General Report On Tunny“ de-klassifiziert. Seither sind fast alle Einzelheiten von COLOSSUS bekannt, freilich nicht dessen weiterhin geheimen kryptanalytischen Algorithmen.

„We go tomorrow!“

Als Eisenhower mit diesen Worten den Startschuss für die Landung gibt, sind in den Wochen vorher durch Bombardierungen und Sabotage möglichst viele Überlandtelefonlinien zerstört worden, um die Deutschen zu zwingen, möglichst viel „intelligence“ per Funkverkehr zu übertragen. Dabei entschlüsselt ULTRA auch einige unangenehme Überraschungen. In der zweiten Hälfte des Monats Mai 1944 wird entdeckt, dass die Deutschen davon ausgehen, dass die Küste zwischen Le Havre und Cherbourg der Hauptlandungsplatz sein würde und daher verstärkt Truppen in die Halbinsel entsenden. Doch diese Erkenntnisse ermöglichen den Alliierten, ihre Landungspläne in der Gegend von Utah Beach anzupassen. Ehe die alliierten Schiffe die Leinen lösen, hat ULTRA Anzahl, Identifikation und Lokalisierung fast aller deutschen Divisionen und Luftstreitkräfte, die genaue Lage der Seeminen, die U-Boot-Einsatzpläne, die Probleme bei Treibstoffversorgung und Truppenverstärkung usw. bestimmt. Die Invasion in der Normandie ist in einem solch engen Zeitrahmen vorgesehen, dass diese nicht ausführbar – oder sogar gescheitert wäre – (wie auch die nachfolgenden Operationen) ohne die genauen und verlässlichen Informationen, die ULTRA mit Hilfe von COLOSSUS über die deutschen Truppen und deren geplanten Operationen liefert.

Fazit

Die alliierten Experten sind bei der Vernehmung der deutschen Kryptologen nach dem Kriege überrascht, dass diese die ganze Zeit darüber im Bild waren, dass die ENIGMA und die Fernschreiber nicht sicher sind und genau wussten, wie diese geknackt werden können. Hier zeigt sich ein weiteres Problem der militärisch dominierten Entscheidungsprozesse: Es sind immer militärische Experten, die sowohl die angebotenen Maschinen prüfen und beschaffen als auch später deren Sicherheit zu beurteilen haben, mithin sich selbst beurteilen. Zusammenfassend ist zu sagen, dass die Offiziere es verstanden, bis zum Kriegsende ihre groben Fehler zu vertuschen, wobei es fraglich ist, ob sie diese überhaupt als solche erkannten.

Hätte die britische Regierung 1945 den Bau von COLOSSUS, dem weltweit ersten digitalen vollelektronischen Rechner bekannt gemacht, dann würde das offizielle Computerzeitalter nicht nach US-Rechnung mit dem ENIAC beginnen. Auch hätten die an COLOSSUS beteiligten britischen Computerpioniere nicht während Jahrzehnten ihren Familien ihre Kriegsarbeit verschweigen und 1996 verbittert miterleben müssen, wie beim ENIAC-Jubiläum ihre wissenschaftliche Pionierarbeit unerwähnt blieb.

Hätten Alan Turing, Gordon Welchman, Harald Keen, Max Newman, Tommy Flowers, Bill Tutte und Zehntausende anderer Mitarbeiter nicht unter größtem persönlichen und unermüdlichen Einsatz während Monaten und Jahren die weltweit einzigartige und größte „intelligence“-Organisation namens ULTRA ermöglicht (und die dann über 40 Jahre totgeschwiegen wurde[5]), der D-Day hätte später stattgefunden (mit fraglichem Erfolg) und der Krieg hätte nicht 1945 geendet. So wären noch Tausende von Menschen in den Fluten des eiskalten Nordatlantik ertrunken und Abertausende auf den Schlachtfeldern und in den Konzentrationslagern eines sich dahinziehenden Krieges zum Opfer gefallen. Diesen Wissenschaftlern und Ingenieuren, Frauen und Männern verdankt die Welt unendlich viel! ■

---

[3] Cobol und Compiler, in DIE WARTE vom 26. Januar 2012.

[4] The PC-User's Guide to Colossus von Benjamin Wells in [1] chapter 10.

[5] Das ULTRA-Geheimnis diente nach dem Krieg weiterhin den Geheimdiensten: Regierungsstellen übergaben „großzügig“ zahlreichen Staaten, darunter auch Nato-Alliierten, erbeutete ENIGMA- und andere Maschinen, die ja damals offiziell sicher waren, zur Verschlüsselung geheimer Sendungen. Und konnten so deren Geheimnachrichten mitlesen. Bekannt wurde auch, dass die offiziell sicheren T52e-Fernschreiber von den französischen und norwegischen Verbündeten verwendet wurden – und dass die COLOSSUS-Maschinen bis in die 60er-Jahre in Betrieb waren, angeblich nur zur Ausbildungszwecken.

Bibliografie: [1] Copeland, B. Jack et al.: Colossus, Oxford 2006; [2] , F.H. Stripp Alan: Code Breakers, Oxford 2001; [3] Pröse, Michael: Chiffriermaschinen und Entzifferungsgeräte im Zweiten Weltkrieg, mpress 2006.