

ALAN TURING

Churchills beste Gans im Stall

Der Enigma-Code der deutschen Wehrmacht im Zweiten Weltkrieg war nicht zu knacken. Doch dann kamen die Dechiffrierer von Bletchley Park – an ihrer Spitze Alan Turing. Zu seinem 100. Geburtstag ein Porträt des Mathematik-Genies

VON Henning Sietz | 24. Mai 2012 - 08:00 Uhr



© Jon Callas/Wikimedia Commons

Alan Turing als Schieferskulptur in den Gebäuden von Bletchley Park.

Ende Juli 1939, wenige Wochen vor Beginn des Zweiten Weltkrieges, stellen sich in Pary bei Warschau einige Briten und Franzosen zu einem ungewöhnlichen Treffen ein. Mitarbeiter des Biuro Szyfrów, des polnischen Chiffrierdienstes, präsentieren den Gästen einen eigenen Nachbau der Chiffriermaschine Enigma, welche die deutsche Wehrmacht benutzt, um Nachrichten zu verschlüsseln. Eine Apparatur namens »Bomba« zum Knacken derselben stellen sie auch gleich vor.

Der polnische Enigma-Nachbau und die Bomba machen Eindruck auf die Gäste. Zwar haben die Franzosen Material über die Enigma an die Polen weitergegeben, doch hielten Franzosen und Briten es bisher für unmöglich, die deutsche Chiffriermaschine zu überlisten. Der polnische Geheimdienst hingegen hat sich nicht entmutigen lassen und – erstmals in der Geschichte der Kryptologie – Mathematiker eingesetzt. Am Vorabend des Zweiten Weltkrieges nun sehen die Polen ihre einzige Chance darin, die verbündeten Briten und Franzosen in ihre Erfolge einzuweihen. Mitte August 1939, wenige Tage vor dem deutschen Überfall, trifft die polnische Enigma mit diplomatischer Post in Paris und London ein.

Die Enigma – das altgriechische Wort bedeutet »Rätsel« – geht zurück auf den Berliner Erfinder Arthur Scherbius (1878 bis 1929), der im Jahre 1923 ein zentnerschweres Chiffriergerät dieses Namens zur geheimen Nachrichtenübermittlung auf dem Kongress

der Internationalen Postunion in Bern vorstellte. Die Resonanz war gering, doch die Reichswehr zeigte Interesse. Sie ließ den klobigen Apparat verbessern und führte das Gerät von 1928 an zum Verschlüsseln ihrer Meldungen ein.

Auf den ersten Blick sieht eine Enigma aus wie eine Schreibmaschine. Das Tastenfeld umfasst die 26 Buchstaben des deutschen Alphabets, ohne Zahlen und Sonderzeichen. Zusätzlich gibt es eine Gruppe von 26 beleuchteten Buchstaben und ein Steckfeld mit 26 Positionen, auf dem sich jeweils zwei Buchstaben per Kabel verbinden und damit vertauschen lassen. Herzstück der Standardausgabe sind drei Rotoren, auch Walzen genannt, die wahlweise auf jeden Buchstaben eingestellt werden können. Drückt man eine Buchstabentaste, läuft ein Stromsignal von der Taste über das Steckfeld zu den Walzen, zurück zu den Steckern und schließlich zum Lampenfeld, wo ein Buchstabe aufleuchtet, der per Hand zu notieren ist. Unterwegs wird der Buchstabe bei jeder Station vertauscht. Tippt man den nächsten Buchstaben, dreht sich die rechte Walze um eine Position weiter, nach einem Durchlauf von 26 Buchstaben rückt auch die mittlere Walze wie bei einem analogen Kilometerzähler um eine Position weiter, zuletzt dann die linke.

Für die britischen Militärs ist der Sonderling ein Albtraum

Theoretisch machte die Enigma ungemein viel her. Drei Walzen mit je 26 Positionen ergaben 17.576 Möglichkeiten. Da sich die Rotoren vertauschen ließen, standen sechs verschiedene Walzenlagen zur Verfügung. Dazu gab es die Steckverbindungen und noch innerhalb jeder Walze einen Ring, den man mit einem Stift verstellen konnte, und zwar auf 26 Positionen. Es war eine weitere Möglichkeit, die Buchstaben zu vertauschen. Dies alles führte zu einer immensen Zahl möglicher Ausgangsstellungen und brachte der Enigma den Mythos ein, unknackbar zu sein.

Dass sie dennoch konstruktive Mängel aufwies, hatten schon die polnischen Mathematiker erkannt. Marian Rejewski untersuchte große Mengen von Tagesmeldungen, die mit ein und demselben Tagesschlüssel chiffriert waren, und stellte Regelmäßigkeiten fest – obwohl jede Meldung einen unterschiedlichen Spruchschlüssel hatte. Auf diese Weise konnte er die innere Verdrahtung der Walzen ermitteln. Weiterhin erkannte er, dass die Walzenstellungen im chiffrierten Text eine Art Fingerabdruck hinterließen. 1938 gelang es dem Biuro Szyfrów, eine Maschine zu konstruieren, ebenjene Bomba, mit der sich durch sechs elektrisch verbundene Walzenlagen Rotoreinstellungen testen ließen. Mit diesem elektromechanischen Brutalverfahren konnte die Mathematikergruppe um Rejewski monatelang Meldungen der Wehrmacht mitlesen.

Die Erfolgsserie brach ab, als Ende 1938 der Tagesschlüssel umgebaut und die Zahl der Walzen, die zur Auswahl standen, auf fünf erhöht wurde (von denen man aber nach wie vor nur drei pro Tag benutzte). Nun hätte das Biuro Szyfrów täglich 60 Walzenlagen testen müssen statt sechs wie bisher. Die polnischen Kryptanalytiker stießen an ihre Grenzen. Sie taten das einzig Richtige und setzten die Alliierten ins Bild.

Sieben Jahre lag Großbritannien zurück, doch es lernte schnell dazu. Die altehrwürdige Government Code & Cipher School (GCCS), die dem Nachrichtendienst MI6 unterstand, wurde im August 1939 als »Station X« nach Bletchley Park verlegt, mitten im Dreieck von London, Oxford und Cambridge. Auch hier sollten Mathematiker die Enigma knacken. Einer von ihnen war Alan Turing vom King's College in Cambridge. Es ist sein Name, der sich heute vor allem mit dem Enigma-Triumph verbindet.

© Wikimedia Commons/Bundesarchiv



Ein deutscher Funker in einem Panzerwagen chiffriert im Mai 1940 mit einer Enigma-Schlüsselmaschine eine Nachricht.

Geboren vor 100 Jahren, am 23. Juni 1912 in London als Sohn eines Beamten des indischen Kolonialdienstes, verlebte Turing seine frühe Kindheit bei Pflegeeltern. Das ABC bringt er sich selbst bei, mit 16 liest er die Schriften Albert Einsteins. In Cambridge, wo

er Mathematik studiert, gilt er als verschroben und schroff. Sein Reden ist oft stotternd, sein Schweigen brüsk. Als guter Brite liebt er Sport. Aber er hasst Konventionen und verbirgt nur nachlässig seine Homosexualität – was gefährlich ist, wird die Liebe zwischen Männern doch streng verfolgt.

Nach einem glänzenden Studium publiziert er 1937 die Schrift *On Computable Numbers*, in der er unter anderem darlegt, dass ein formales Gerät – das später »Turing-Maschine« genannt werden sollte – jede mathematische Aufgabe lösen kann, sofern sie durch einen Algorithmus darzustellen ist. Mit dieser Schrift, einer der Grundlagen der theoretischen Informatik, hat er den Computer entworfen.

Im Sommer 1938 erreicht ihn eine Anfrage der GCCS, ob er sich in Kryptologie ausbilden lassen würde. Am 4. September 1939 – seit einem Tag herrscht Krieg zwischen Deutschland und England – trifft er in Bletchley Park ein, kurz darauf überträgt man ihm die Leitung einer Gruppe von Mathematikern in Baracke 8, die den Code der deutschen Kriegsmarine entschlüsseln soll .

Trotz der polnischen Arbeit stehen die Mathematiker im Herbst 1939 vor einem Neuanfang. Dadurch, dass es jetzt fünf Walzen gibt, die zur Auswahl stehen, sind die polnischen Erkenntnisse mit einem Schlag Makulatur geworden.

Nun gibt es für die einzelnen Waffengattungen und auch Regionen verschiedene Enigma-Geräte und Codes. Während die Briten beim Code für die Luftwaffe bald große Fortschritte machen, kommen sie bei der Marine nicht weiter. Im Frühjahr 1940 wird die Lage prekär. Das Reich baut die U-Boot-Flotte aus, um Großbritannien von der Versorgung über den Atlantik abzuschneiden. Es ist ein Angriff auf die Lebensader des Landes.

Neue Ideen müssen her. Turing versucht es mit der Methode des wahrscheinlichen Wortes, die er perfektioniert: Wenn man eine vermutete Wendung (»An den General«) aus einer Meldung exakt mit den entsprechenden Chiffrebuchstaben in Relation setzt, lassen sich Zyklen aufstellen, die getestet werden können, bis man irgendwann deutschen Text erhält – und damit auch den Tagesschlüssel. Bei dem stereotypen Charakter der Meldungen sollte es nicht allzu schwer sein, solche Textstücke, *cribs* genannt, zu konstruieren. Deutsche Wetterschiffe, deren Nachrichten ebenfalls per Enigma verschlüsselt werden, senden eben nichts anderes als Wetterdaten, in feststehenden Ausdrücken. Mit Papier und Bleistift ist das indes nicht zu schaffen, dazu braucht man Maschinen – neue »Bomben«, wie sie im Jargon heißen.

Das Problem ist das Steckbrett; *steckerboard* nennen es, deutsch-englisch, die Mathematiker von Bletchley Park. Die mithilfe der Kabel erzielten Buchstabenvertauschungen müssen für jede Rotorposition durchgespielt werden. Um das zu erreichen, stellt Turing ein System von logischen Schleifen auf, die durch Bestätigung oder Widerspruch von Hypothesen Steckverbindungen ermitteln oder ausschließen. Diese Schleifen gilt es in die Schaltkreise einzubauen, deren Relais die »Bomben« steuern sollen.

Im Frühjahr 1940 konstruiert eine Büromaschinenfirma in Letchworth die ersten dieser Apparate. Jede entspricht 36 Enigmas zu je drei Rotoren, eingebaut in einen Schaltschrank.

Doch sie laufen entsetzlich langsam. Daraufhin hat der Mathematiker Gordon Welchman, Turings Kollege aus Cambridge, eine bestechende Idee. Das endlose Abarbeiten der Schleifen lasse sich durch eine einfache Implikation abkürzen: Wenn die Enigma »M« in »O« verschlüsselt, muss sie mit derselben Einstellung auch »O« in »M« verwandeln. Ist das nicht gegeben, sind die Rotorpositionen falsch. So können auf einen Schlag Millionen falscher Hypothesen ausgeschlossen werden. Als »Diagonalplatine« wird die geniale Idee in die Schaltkreise und Relais der »Bombe« eingearbeitet. Im August 1940 liefert Letchworth die verbesserten Anlagen, wahre Meisterwerke der Mechanik. Nun kommt man mit kürzeren *cribs* aus.

Die »Turing-Welchman-Bomben« stehen außerhalb von Bletchley Park und werden von Angehörigen des Women's Royal Naval Service bedient, den »Wrens«. Tag und Nacht stellen Hunderte der Wrens, meist junge Frauen, die Apparate ein und beaufsichtigen ihren Lauf. Die Luft in den Räumen ist heiß und stickig, es riecht nach Öl, jeden Moment kann es wieder einen Kurzschluss geben. Pausenlos klicken die Relais, Tausende Bürsten aus Klavierdraht surren über die elektrischen Kontakte. Stoppt eine Maschine, geben Wrens die Einstellung per Telefon an Bletchley Park durch, wo sie an einer Enigma ausprobiert wird. Oft genug ist es ein Fehlalarm. Jede Nacht um null Uhr geht die Jagd auf den Tagesschlüssel der Enigma von Neuem los.

Bis zuletzt begreift die Wehrmacht nicht, was gespielt wird

Baracke 8 ist ein erlesener Verein von Mathematikern. Unter ihnen ist Alan Turing der »Prof« – hoch geachtet als Kryptanalytiker, im Übrigen aber ein großer Junge und Sonderling. Er findet nichts dabei, in Pyjamajacke unter dem Sportsakko angeradelt zu kommen, auch mit Gasmasken, wenn Pollenflug herrscht. Seinen Teepott, im Krieg unersetzlich, pflegt er am Heizungsrohr anzuketten. Gern rezitiert er skurrile Verse, etwa aus Disneys *Schneewittchen* -Film den Zauberspruch der bösen Königin, als sie den Apfel ins Gift taucht: »*Dip the apple in the brew, / let the sleeping death seep through*« (»Tunk den Apfel ins Gebräu, / lass den stillen Tod herbei«). Für die Staboffiziere in Bletchley Park ist er ein »militärischer Albtraum«, wie der britische Mathematiker Andrew Hodges 1983 in seiner Turing-Biografie festhielt.

Der Erfolg stellt sich zögernd ein. Es zeigt sich, dass gute *cribs* schwerer als erwartet zu finden sind. Noch im März 1941 ist kein einziger Funkspruch der Kriegsmarine lesbar, April und Mai sind bessere Monate, aber die Entschlüsselungen dauern viel zu lange. Erst Ende Mai schafft Baracke 8 den Anschluss. Nun liegen die dechiffrierten Informationen, genannt »ULTRA«, nur noch einen Tag zurück.

Die Erfolge von Baracke 8 hängen am seidenen Faden: Eine einzige Änderung, und alles ist wieder zunichte. Man braucht dringend Enigma-Unterlagen, deutsches Originalmaterial.

So setzt die Royal Navy trotz der strengen Geheimhaltung alles aufs Spiel und kapert einige deutsche Wetterschiffe. Im März 1941 trifft es den Trawler *Krebs*, im Mai werden das Wetterschiff *München* und die *U-110* aufgebracht. Die Beute: verschiedene Schlüssellisten der Enigma. Jede Kaperung hätte das Misstrauen der Wehrmacht erregen können, doch niemand schöpft Verdacht. Mit den Trophäen kann Bletchley Park vom Frühsommer 1941 an die Funksprüche der Kriegsmarine mitlesen.

Ende Mai gelingt es den Briten, im Nordatlantik den Stolz der Nazi-Marine zu versenken, die erst im Jahr zuvor in Dienst gestellte *Bismarck*. Dass auch sieben *Bismarck*-Versorgungsschiffe zerstört werden, verdankt die Royal Navy Bletchley Park. In der zweiten Jahreshälfte 1941 kann sie die Geleitzüge um die lauernden U-Boote herumlenken, der Verlust an alliiertem Schiffsraum geht stark zurück, obwohl Deutschland mehr und mehr U-Boote in den Atlantik schickt. Der Erfolg ist hart erarbeitet: Pro Tag fallen in Bletchley Park rund 3.000 Nachrichten an, die abgehört, erfasst, analysiert, dechiffriert, übersetzt, militärisch eingeschätzt und bewertet werden. Die Masse der Informationen zu bewältigen ist das eigentliche Problem. Im September 1941 kommt Premier Winston Churchill zu Besuch, um den »Gänsen, die goldene Eier legen – und nicht schnattern«, eine patriotische Rede zu halten. In Baracke 8, wo sich das Schicksal des Landes entscheiden sollte, wird ihm ein nervöser Alan Turing vorgestellt. Den Namen merkt er sich.

Die Katastrophe kommt mit dem 1. Februar 1942: Die Kriegsmarine erhöht die Zahl der permanenten, täglich benutzten Walzen von drei auf vier. Damit steigt die Zahl der möglichen Walzenpositionen um das Sechszwanzigfache. Von einem Tag auf den anderen bricht der Fluss der Nachrichten in Bletchley Park ab. Die Folgen sind dramatisch: Immer mehr U-Boote jagen im Atlantik, im Januar 1942 sind es rund hundert, im Oktober bereits 196, Ende 1942 schließlich 212. Pro Monat verlieren die Alliierten rund 500.000 Tonnen Schiffsraum – mehr, als sie bauen können.

Nun machen die USA Druck. Ihre Mathematiker haben den japanischen Code geknackt. Ihre »Bomben« laufen besser und schneller als die der Briten. Präsident Franklin D. Roosevelt drängt Churchill zur Zusammenarbeit. Fortan wird jeder ermittelte Tagesschlüssel dem Partner unverzüglich mitgeteilt. Im November 1942 reist Turing – vermutlich auf Churchills Vermittlung – nach New York, um die amerikanischen Kollegen in die britischen Methoden einzuweisen. Die Reise markiert Turings Abschied von der Baracke 8, bei seiner Rückkehr im Frühjahr 1943 muss er feststellen, dass man auch ohne ihn zurechtkommt. Er ist jetzt Berater. Hat man den Sonderling auf elegante Weise loswerden wollen?

Am 30. Oktober 1942 wendet sich das Blatt: Im Mittelmeer, vor Port Said, kann die Royal Navy das deutsche U-Boot *U-559* aufbringen und mehrere Schlüssellisten bergen. Wieder einmal hilft die Kriegsmarine den Alliierten durch schwere Fehler im Funkverkehr, indem sie einen Tag lang nur mit drei Rotoren chiffriert und zudem die Walzen falsch verwendet, sodass eine Kauderwelsch-Meldung korrekt wiederholt werden muss – für Bletchley Park

ein gefundenes Fressen. Nach Wochen harter Arbeit hat es Baracke 8 erneut geschafft: Allmählich lassen sich die U-Boot-Positionen im Atlantik ermitteln, sodass die Geleitzüge wieder um die deutschen U-Boote herumgeführt werden können. Und endlich greifen auch die neuen technischen Entwicklungen der Alliierten: Langstrecken-Aufklärer mit Radargeräten überwachen den gesamten Nordatlantik, mithilfe von Kurzwellenpeilungen lassen sich U-Boote entdecken. Vom Frühjahr 1943 an werden die Jäger zu Gejagten, wenige Monate später haben die Alliierten die Materialschlacht im Atlantik gewonnen.

Dass die Erfolge der Briten die Wehrmacht zu keiner Zeit an der Enigma zweifeln ließen, ist vielleicht die erstaunlichste Tatsache im Krieg der Chiffren. Nicht einmal der Umstand, dass die U-Boote kaum noch Geleitzüge entdecken konnten, erregte Verdacht. Das Oberkommando der Wehrmacht glaubte felsenfest an Spionage in den eigenen Reihen.

Unmittelbar nach Kriegsende ließ Churchill Bletchley Park auflösen. Die rund 9.000 Mitarbeiter wurden entlassen, die Dechiffriermaschinen zerstört, die Unterlagen vernichtet. Turing war jetzt Officer of the Order of the British Empire, den Orden versenkte er in seiner Werkzeugkiste.

Er verfolgte weiterhin sein großes Ziel, ein elektronisches Gehirn zu bauen. Am National Physical Laboratory konstruierte er den Computer ACE (Automatic Computing Engine), einen der ersten britischen Rechner. 1948 wechselte er an die Universität Manchester, wo er den Computer »Manchester Mark 1« programmierte.

Anfang 1952 dann der Beginn der Tragödie. Ein Gelegenheitsdieb bricht in sein Haus ein. Bei den Ermittlungen gibt Turing zu, homosexuelle Kontakte zu einem Mann gehabt zu haben, der sich als Komplize des Einbrechers entpuppt. Die Reaktion ist gnadenlos: Der Richter lässt Turing die Wahl zwischen einer Gefängnisstrafe oder einer Chemotherapie mit Östrogen, die seinen Sexualtrieb unterdrücken soll. Turing entscheidet sich für die Therapie. Am 8. Juni 1954 findet man ihn tot in seinem Haus in Wilmslow bei Manchester, neben ihm liegt ein Apfel, von dem er abgebissen hat. Ein feiner Geruch von Bittermandel hängt im Raum, Anzeichen für Zyankali.

Wie heißen sie doch, die Verse, die er so gern zitiert hat? *»Dip the apple in the brew, / let the sleeping death seep through!«*

COPYRIGHT: ZEIT ONLINE

ADRESSE: <http://www.zeit.de/2012/22/Turing-Enigma>