Zweiter Weltkrieg: Informationskrieg

Kapitel 4: Entschlüsselung

**Die Entzifferung der Geheimschriften**

Ein Bild, das Schreibmaschine enthält.

Automatisch generierte Beschreibung

Foto: Punishar

[Wikimedia Commons](https://commons.wikimedia.org/wiki/File:Enigma_05.jpg)

«Mit einer solchen Maschine können wir alle geheimen Befehle sicher funken; auch wenn die feindlichen Geheimdienste die Signalsprüche abfangen, aus dem Buchstabensalat können sie nicht auf die richtige Meldung kommen», dachten sich die deutschen Spezialisten.

Was sie nicht wussten: Bereits 1932, sieben Jahre vor dem Krieg, hatte ein genialer polnischer Mathematiker die Enigma-Verschlüsselung geknackt: Marian Rejewski (1905–1980) erkannte, dass es in der scheinbaren Regellosigkeit der Buchstabenfolgen doch Auffälligkeiten gab. Beispielsweise setzten die Chiffreure für einen Leerraum zwischen zwei Wörtern immer ein x ein; ferner verdoppelten sie wichtige Wörter, so dass Rejewski, wenn er deren Stelle erriet, herausfinden konnte, wie die Rotoren verdrahtet waren. Dies war vor allem am Anfang einer Meldung der Fall, denn dort musste in einer Dreiergruppe von Buchstaben angegeben werden, in welche Ausgangsstellung die Rotoren bei der Entschlüsselung einer Botschaft gebracht werden mussten. Und weil die Chiffreure diese Angabe für so wichtig hielten, funkten sie diese Dreiergruppe gleich zweimal hintereinander. Der geniale Rejewski hatte die Enigma schon vor dem Krieg geknackt und gab seine Erkenntnisse nach dem Überfall auf Polen den französischen und englischen Spezialisten weiter.

Vor allem diese konnten so auch Veränderungen an den Enigma-Maschinen weiter nachverfolgen. Anhand der Funksprüche wussten sie, wohin im Atlantik die deutschen Unterseeboote kommandiert wurden – und die englischen und amerikanischen Schiffe konnten ihnen ausweichen. Aber auch bei der Invasion an der Normandie am 6. Juni 1944 waren den Alliierten die deutschen Stellungen bekannt.

Vor allem gelang es den Alliierten das Geheimnis, den Code geknackt zu haben, bis zum Ende des Zweiten Weltkrieges zu bewahren. Sie nahmen bisweilen sogar Verluste an Schiffen in Kauf, um dem Feind nicht einen Hinweis zu geben, dass sie seine Pläne durchschaut hatten! Ja, noch über das Kriegsende hinaus behielten sie das Staatsgeheimnis für sich, erst dreissig Jahre später, 1974, berichteten sie darüber.

Übrigens ging es den Alliierten mit ihren Verschlüsselungssystemen nicht viel besser: die deutschen Spezialisten knackten bereits 1939 und 1940 den Code der britischen Marine und 1942–1944 denjenigen der amerikanischen Diplomaten. Die amerikanischen Spezialisten kannten bereits 1940, noch vor dem Krieg mit diesem Staat, den japanischen Code. Alle Erfolge hatten eine Ursache gemeinsam: die Unvorsichtigkeit bei der Codierung erlaubte Aufschlüsse. Und die Erfolge während des Krieges hatten noch eine zweite Ursache: Die Entwicklung von Rechenmaschinen, die schon in vergleichsweise kurzer Zeit die noch verbliebenen Buchstabenkombinationen durchsuchen und auf sinnvolle Wörter hin überprüfen konnten. Der Kampf um die Informationen führte zur Entwicklung der ersten Computer!

Aufgabe: Ein Problem der Enigma bestand auch darin, dass sie wegen des Rotorsystems «zuverlässig» jeden Buchstaben durch einen andern ersetzte. Hatte man eine Vermutung, dass ein bestimmtes Wort vorkam, konnte man zuverlässig ermitteln, wo. Wo?

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Verschleierte Meldung |  | G | O | B | X | T | O | U | F | O | T | A |
| Wo steckt das Wort ‹Uboot›? | 1 | u | b | o | o | t |  |  |  |  |  |  |
| 2 |  | u | b | o | o | t |  |  |  |  |  |
| 3 |  |  | u | b | o | o | t |  |  |  |  |
| 4 |  |  |  | u | b | o | o | t |  |  |  |
| 5 |  |  |  |  | u | b | o | o | t |  |  |
| 6 |  |  |  |  |  | u | b | o | o | t |  |
| 7 |  |  |  |  |  |  | u | b | o | o | t |

**Lösung und Erläuterungen**

Die Aufgabe zeigt ein Problem von Chiffriermaschinen auf: Je mehr sie verschlüsseln wollen, umso eher lassen sie wieder eine Lücke offen: Wenn man jeden Buchstaben verschlüsselt, erleichtert man die Entschlüsselung, weil man nur noch unter 25 statt unter 26 Buchstaben nach dem originalen suchen muss! In der Fachsprache der Kryptologie spricht man von «complication illusoire».

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Verschleierte Meldung |  | G | O | B | X | T | O | U | B | E | T | A |
| Wo steckt das Wort ‹Uboot›? | 1 | u | b | o | o | **t** |  |  |  |  |  |  |
| 2 |  | u | **b** | o | o | t |  |  |  |  |  |
| 3 |  |  | u | b | o | **o** | t |  |  |  |  |
| 4 |  |  |  | u | b | **o** | o | t |  |  |  |
| 5 |  |  |  |  | u | b | o | o | t |  |  |
| 6 |  |  |  |  |  | u | b | o | o | **t** |  |
| 7 |  |  |  |  |  |  | u | **b** | o | o | t |

In den Varianten 1 bis 4 und 6 und 7 kann das Wort nicht stecken, weil dort ein Buchstabe (der fettgedruckte) nicht verschlüsselt worden wäre. Also ist nur die Variante 5 möglich. Hier ist jeder Buchstabe ein anderer als in der verschleierten Meldung.

Mit dieser einfachen Aufgabe wird nur eine winzige Fazette der Algorithmen zum Entschlüsseln des Enigma-Codes dargestellt. Wichtig waren viele weitere, komplizierte Operationen mit computerähnlichen Maschinen (so genannten «Bomben») und Denkleistungen – 10'000 Menschen arbeiteten allein in Grossbritannien an der Entschlüsselung. Aber auch handfeste Enter-Aktionen zur See brachten die Briten in den Besitz von Enigma-Unterlagen, während die Geräte selbst in allen Fällen über Bord geworfen worden waren.

Eine besonders pikante Seite besteht darin, dass auch die Schweiz von Deutschland 260 Enigma-Maschinen bezogen und die Verdrahtung in einzelnen Rotoren etwas abgeändert hatte. Trotzdem haben während des Zweiten Weltkrieges deutsche, polnische, britische und amerikanische Spezialisten die Schweizer Enigma entschlüsselt. Die Geräte wurden bis in die achtziger Jahre noch als Reserve verwendet und 1994 die letzten versteigert.