Die Arbeit der Kryptoanalytiker

Die Verschlüsselung und Entschlüsselung von Nachrichten, die in Friedenszeiten gleichermaßen wie in Kriegszeiten praktiziert wird, ist so alt wie die Nachrichtenübertragung selbst. Das gegenseitige Belauschen und der Versuch des Entschlüsselns von Funknachrichten gehörten folgerichtig von Beginn an zum Instrumentarium aller Kriegsparteien des 2. Weltkrieges. Lange Zeit vor der Öffentlichkeit verborgen blieb die Quantität und die Qualität der Verschlüsselungsarbeit der Government Code and Cypher School in Bletchley Park (B.P.), einem unscheinbaren Landsitz 70 km nordwestlich von London.

Mit Ausbruch des Krieges setzten hier britische Kryptoanalytiker alles daran, den geheimen Funkverkehr der Wehrmacht zu entschlüsseln, was über weite Strecken gelang, wie heute bekannt ist. Allgemein anerkannt ist die Tatsache, dass insbesondere die 4-Walzen-Ausführung, wie sie auch in Erfurt hergestellt wurde, schwierig zu entschlüsseln war. Dabei kam es darauf an, die empfangenen Nachrichten in möglichst kurzer Zeit zu entschlüsseln, da ihr militärischer Inhalt sonst wertlos wurde.

Es gab begünstigende Faktoren, die den britischen Codebrechern die Arbeit erleichterten, die aber den hohen personellen und technischen Aufwand nicht überflüssig machten. Dazu gehörte die Vorarbeit von französischen und polnischen Mathematikern, die vor dem Krieg an der Entschlüsselung der 3-Walzen-Enigma arbeiteten und die im Juli 1939 ihre Kenntnisse den britischen Spezialisten mitteilten.

Hilfreich war auch das Erbeuten einiger Enigma-Geräte während des Krieges. Ohne die zugehörigen Schlüsseltabellen gelingt allerdings keine sofortige Entschlüsselung. Entscheidend für eine kurzfristige und weitgehend lückenlose Entschlüsselung der abgehörten Funksprüche war die von den britischen Mathematikern Alan Turing (1912 – 1954) und Gordon Welchman (1906 – 1985) entwickelte „Turing-Welchman-Bombe“.

Diese elektromechanische Maschine besteht aus der Reihenschaltung von 3 x 12 Walzensätzen der Enigma. Die Walzen drehen sich mit einer Geschwindigkeit von 64 Umdrehungen pro Minute. Eine angenommene Textphrase wird mit den möglichen Walzenstellungen verglichen, bis eine Übereinstimmung gefunden wird