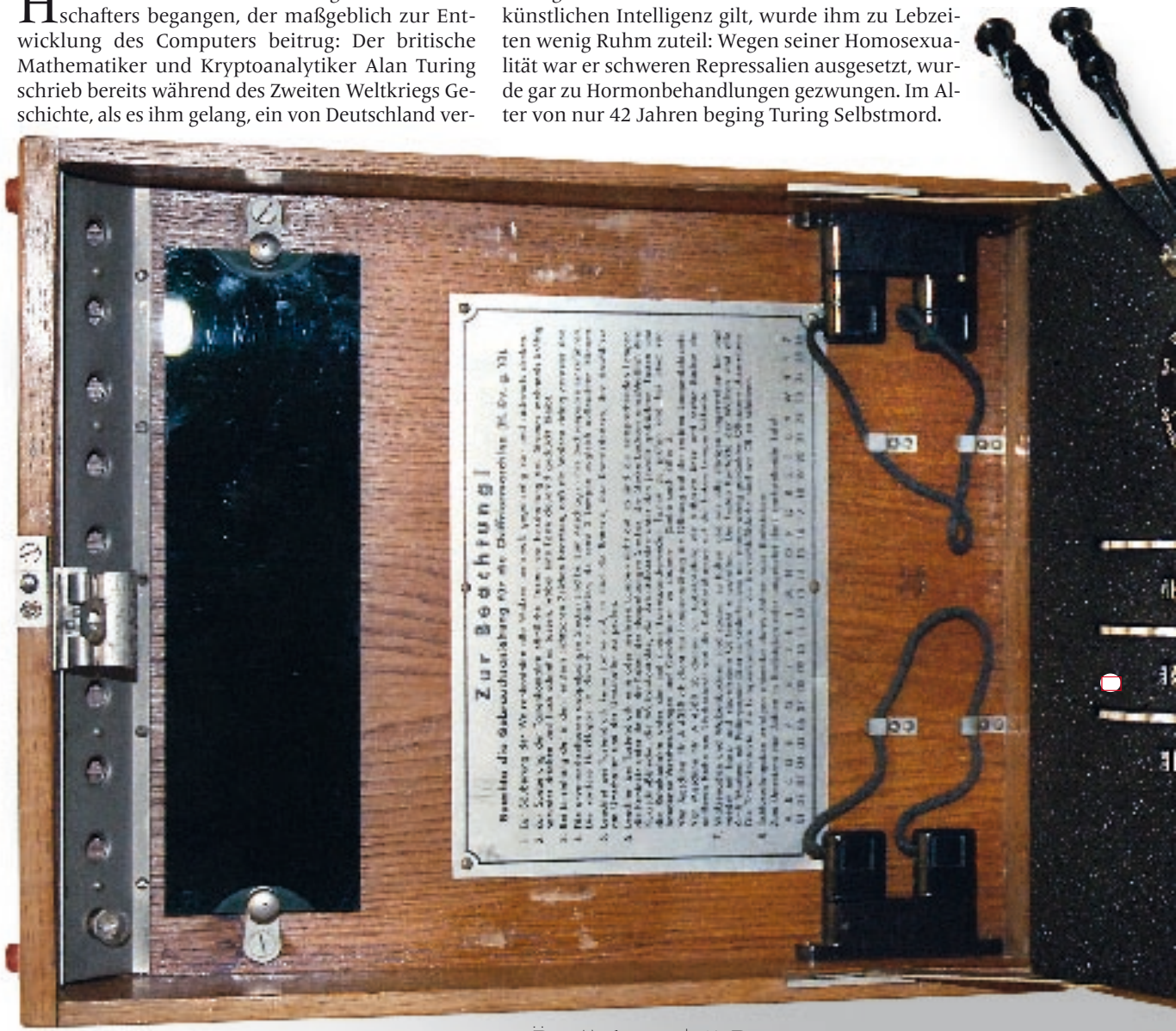
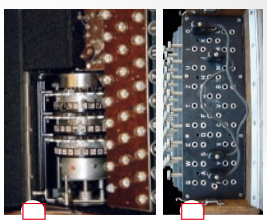
Codename Enigma

Heuer wird der 100. Geburtstag eines Wissenschafters begangen, der maßgeblich zur Entwicklung des Computers beitrug: Der britische Mathematiker und Kryptoanalytiker Alan Turing schrieb bereits während des Zweiten Weltkriegs Geschichte, als es ihm gelang, ein von Deutschland verwendetes Verschlüsselungssystem zu knacken – die Chiffriermaschine Enigma, zu Deutsch Rätsel. Turing ersann ein Entschlüsselungsprinzip, „Turing-Bombe" genannt, mit dem wichtige Nachrichten abgefangen werden konnten, was aus heutiger Sicht wesentlich zum Sieg der Alliierten beitrug. Obwohl Turing als Gründervater der Informatik und der künstlichen Intelligenz gilt, wurde ihm zu Lebzeiten wenig Ruhm zuteil: Wegen seiner Homosexualität war er schweren Repressalien ausgesetzt, wurde gar zu Hormonbehandlungen gezwungen. Im Alter von nur 42 Jahren beging Turing Selbstmord.

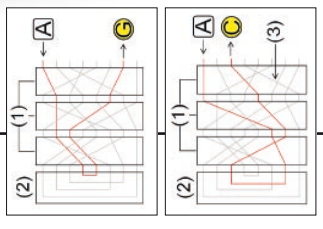
ALAN TURING
1912 bis 1954



DAS ENIGMA-PRINZIP
Auf den ersten Blick gleicht Enigma einer Schreibmaschine. Sie besteht aus einer □ Tastatur, □ drei Walzen, einem □ Lampenfeld sowie dem so genannten □ Steckerbrett.

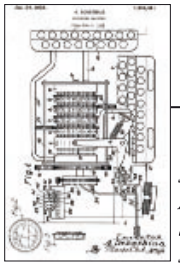


DIE CODIERUNG
Auf der Verdrahtung der Walzen (1) beruht die Chiffrierung: Drückt man auf der Tastatur etwa den Buchstaben A, fließt Strom zum Eingangskontakt A in der rechtesten Walze (3). Weil Eingangskontakt A mit einem anderen Ausgangskontakt verkabelt ist, kommt es zu einer Vertauschung des Buchstabens. Dies geschieht in allen drei Walzen, bis die Umkehrwalze (2) erreicht wird. Diese vertauscht die Buchstaben ein weiteres Mal und schickt den Strom dann zurück – wobei nochmals drei Vertauschungen stattfinden. Der Strom verlässt die rechteste Walze beispielsweise durch den G-Kontakt.



DER BLICK INS INNERE

Herzstück sind drei drehbare Walzen mit jeweils den 26 Buchstaben des Alphabets. Auf beiden Seiten der Buchstaben befindet sich jeweils ein elektrischer Kontakt, durch elektrische Drähte verbunden. Ähnlich einem Kilometerzähler schalten die Walzen bei jedem Tastendruck weiter. Jeder Buchstabe wird anders verschlüsselt.



1918 Der deutsche Ingenieur Alfred Scherbius lässt die Verschlüsselungsmaschine Enigma patentieren. Zunächst wird sie zivil genutzt.

1934 Die Benutzung von Enigma durch die deutsche Wehrmacht beginnt.

1939 bis 1945: Unter dem Codenamen „Ultra" entschlüsseln die Briten am Landsitz Bletchey Park täglich etwa 2500 Nachrichten der Wehrmacht und der Luftwaffe. Rund 10.000 Menschen sind während des Kriegs dort beschäftigt.

1943 Alan Turing entwickelt für das britische Militär die Entschlüsselungsmaschine Turing-Bombe.

1943 Immer mehr deutsche U-Boote werden durch die Alliierten versenkt, weil mithilfe der Turing-Bombe deren Positionen entschlüsselt werden können.

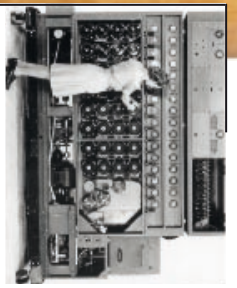
1945 bis 1950: Die Briten zerstören den Großteil ihrer Turing-Bomben, um das Geheimnis der Enigma-Entschlüsselung zu wahren. Erst in den siebziger Jahren erfährt die Öffentlichkeit, dass Enigma bereits während des Kriegs geknackt wurde.

DER SCHLÜSSELTEXT

Im Steckerbrett kann eine weitere Vertauschung der Buchstaben stattfinden. Am Lampenfeld leuchtet schließlich der „Schlüsseltext" auf. Wenn die Enigma komplett verschlüsselt ist, gibt es 10.114 mögliche Anordnungen. Die Deutschen ließen zur Entzifferung der Nachrichten einen so genannten Tagesschlüssel kursieren.

DER CODE-KNACKER

Die Turing-Bombe besteht im Wesentlichen aus zahlreichen kombinierten Enigmas und tastet systematisch alle denkbaren Kombinationen ab. Ein wichtiges Prinzip dabei ist die Wahrscheinlichkeit – unwahrscheinliche Worte werden systematisch ausgeschlossen, wahrscheinliche nach und nach eingegrenzt. Dieser frühe „Computer" war maßgeblich für die weitere Entwicklung der Informatik.



CODEBLATT BONN; MAXIMILIAN SCHÖNHERR; MESSNER WOLAND; NSA; US PATENT; 1928; PICTUREDESK.COM