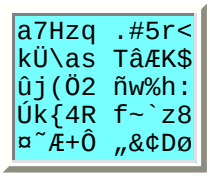
Kryptologie

Die Enigma



Beschreibungen, Artikel, Simulationen

- Historical Ciphers (Linksammlung von Joe Peschel).
- The Enigma.
- Basic Principles of the Enigma (John Savard).
- CFD Hosts Lecture on Enigma.
- Enigma.
- How the Enigma Works (by Alan Stripp).
- Die Abwehr-Enigma (by David Hamer).
- Enigma Photos for Download.
- Turing's Treatise on Enigma.
- German Army Enigma Message.
- James J. Gillogly: Ciphertext-only Cryptanalysis of Enigma. Cryptologia XIX/4 (1995). Kommentare dazu.
- The Influence of ULTRA in the Second World War (Harry Hinsley).
- Decoding Nazi Secrets (Nova online).
- Work by the Poles to break Enigma codes.
- The Alan Turing Home Page (Andrew Hodges)

Historische Daten

- Gründung der »Chiffriermaschinen AG« durch Scherbius.
  Angebot Enigma A, B als ziviles, kommerzielles Chiffriersystem;
  4 Rotoren (»Durchgangsräder«).
- 1926 Willi Korn: Patentanmeldung »Umkehrwalze« → Enigma C.
- 1927 Enigma D mit einstellbarer Umkehrwalze.
- 1933 Auflösung der »Chiffriermaschinen AG«;
  Neugründung der »Chiffriermaschinen-Gesellschaft Heimsoeth und Rinke« (bis 1945).
  Weiterentwicklung zu militärischem Chiffriergerät (Enigma I, »Wehrmachts-Enigma«).
  Einführung des »Steckerbretts«.
- 1938-1942: Enigma K an Schweizer Armee verkauft.
- 1942 Version M4 für die Marine mit zusätzlichem Rotor.
- Nach dem Krieg Verkauf der erbeuteten Maschinen an Entwicklungsländer; im Gebrauch bis ca. 1975.

Ausländische Varianten

- ca. 1928 britische Variante: TYPEX.
- Polnische Variante: Lacida.
- Japanische Variante: »GREEN«.
- US-Variante M-235 = SIGFOY von Friedman.
- 1946 NEMA für Schweizer Armee mit 6 Rotoren.
- NATO-Chiffriergerät KL-7 [extern].

- Variante mit 7 Rotoren von OMI (Ottico Meccanica Italiana).

Besonderheiten der Enigma

Von den verschiedenen Versionen wird hier die »Wehrmachts-Enigma« beschrieben.

- Es werden $q = 3$ Walzen (Rotoren) aus einem Walzenkorb der Größe $p = 5$ ausgewählt.
- Der Strom fließt von rechts durch die drei Rotoren, dann durch die Umkehrwalze, dann in umgekehrter Richtung wieder durch die drei Rotoren nach rechts wie hier von John Savard skizziert.
- Die Umkehrwalze (oder »Reflektor«)
  - dreht sich nicht,
  - verdoppelt die Anzahl der durchlaufenen Rotoren,
  - macht die gesamte Verschlüsselung involutorisch, d. h., Verschlüsselungs- und Entschlüsselungsfunktion sind identisch,
  - ermöglicht dem Kryptoanalytiker eine negative Mustersuche, da niemals ein Buchstabe durch sich selbst verschlüsselt wird.
- Die drei Rotoren werden im wesentlichen nach dem Zählwerkprinzip weitergeschaltet; der rechte, also erste und letzte Rotor im Stromlauf, ist der schnelle, der linke, an die Umkehrwalze grenzende, der langsame. Es gibt eine kleine Unregelmäßigkeit: Immer, wenn sich der langsame Rotor dreht, schiebt er den mittleren noch eine Position weiter, so dass dieser eine ganze Umdrehung schon nach 25 Schritten schafft.
- Die Beschriftung jedes Rotors ist auf dem »Alphabetring« angebracht, der den Rotor umschließt und sich frei auf diesem drehen läßt. Da die Mitnehmer für die Zählwerk-Schaltung am Alphabetring befestigt sind, wird dadurch deren Stellung veränderlich und beeinflusst die Zustandsänderungsfunktion g. Das ergibt einen zusätzlichen Schlüssel, die »Ringstellung«.
- Die Zuordnung der Tastatur bzw. der Lämpchen zum Eingang des rechten Rotors wird über ein Steckerbrett geführt; jeder der 10 gesetzten Stecker vertauscht ein Buchstabenpaar. Das Steckerbrett bewirkt also eine zusätzliche Involution auf der Input- wie auf der Output-Seite. Das ergibt nochmal einen zusätzlichen Schlüssel, die »Steckerverbindungen«.

Bilder der gesamten Maschine sind hier (Wehrmachts-Enigma) oder hier (Marine-Enigma) oder extern, bei NOVA, zu sehen.

Laut Dienstvorschrift durften bei der Wehrmacht verschlüsselte Nachrichten nicht länger als 250 Zeichen sein - längere Texte mussten aufgeteilt und mit verschiedenen Spruchschlüsseln chiffriert werden.

Der Schlüsselraum

Es gibt

- $5!/2! = 60$ Walzenlagen,
- $26^3 = 17576$ Ringstellungen,
- $26!/(2^{10} \cdot 10! \cdot 6!) = 150\,738\,274\,937\,250$ Möglichkeiten für die Steckerverbindungen [siehe unten],
- $26^3 = 17576$ Anfangsstellungen.

Der gesamte Schlüsselraum K (Primär- und Sekundärschlüssel) hat also die Größe

$$\#K = 60 \cdot 17576 \cdot 150\,738\,274\,937\,250 \cdot 17576 = 2\,793\,925\,870\,508\,516\,103\,360\,000 \approx 2.8 \times 10^{24} \approx 1.16 \times 2^{81}.$$

Da aber überhaupt nicht klar ist, ob alle Schlüssel verschiedene Substitutionen definieren, kann man daraus nur schließen, dass die effektive Schlüssellänge höchstens ungefähr 81 ist.

Die Anzahl der Involutionen

Die oben behauptete Anzahl der Möglichkeiten für die Steckerverbindungen bedarf noch einer Begründung. Es handelt sich dabei um die Anzahl der Involutionen in $\mathbf{S}_{26}$ mit höchstens 10 Zweierzyklen.

Allgemein bestimmen wir die Anzahl der Involutionen in der symmetrischen Gruppe $\mathbf{S}_n$ mit höchstens k Zweierzyklen, wobei $0 \le 2k \le n$. Sie ist gleich der Anzahl $d(n,k)$ der Möglichkeiten, k Paare aus n Elementen zu wählen.

Wahl von	# Möglichkeiten	Wahl von	# Möglichkeiten
1. Element:	n		
1. Partner:	n-1	1. Paar:	$n(n-1)/2$
2. Element:	n-2		
2. Partner:	n-3	2. Paar:	$(n-2)(n-3)/2$
…	…	…	…
k. Element:	n-2(k-1)		
k. Partner:	n-2(k-1)-1	k. Paar:	$(n-2k+2)(n-2k+1)/2$

Insgesamt ergibt das mit Berücksichtigung der Reihenfolge

$$n(n-1)\cdots(n-2k+2)(n-2k+1)/2^k$$

Möglichkeiten. Davon sind, wenn man nun die Reihenfolge außer Acht lässt, jeweils $k!$ identisch. Die gesuchte Anzahl ist also

$$d(n,k) = n!/[2^k k!(n-2k)!]$$

Im Falle der Wehrmachts-Enigma ist $n = 26$ und $k = 10$, so dass die oben angegebene Anzahl berechnet ist.

Die Steuerlogik

Üblicherweise wird der schnelle Rotor mit 1, der mittlere mit 2 und der langsame mit 3 bezeichnet. Nach der obigen Beschreibung ist die Zustandsänderungsfunktion also

$$g(z_1, z_2, z_3) = (z_1+1,\ z_2+\lambda(z_1)+\lambda(z_1)\lambda(z_2),\ z_3+\lambda(z_1)\lambda(z_2))$$

mit $\lambda(x) = \delta_{x,25}$ (Kronecker-Symbol).

Die Periode ist also 26·25·26 = 16900.

Die Enigma-Gleichung

Die drei beweglichen Rotoren, die zunächst von rechts nach links durchquert werden, werden in dieser Reihenfolge nummeriert. Ihr Zustand wird dann durch einen Vektor

$$z = (z_3, z_2, z_1)$$

beschrieben. Die zugehörige Rotorsubstitution werde mit

$$\sigma_z = \rho_3^{(z_3)} \circ \rho_2^{(z_2)} \circ \rho_1^{(z_1)}$$

bezeichnet. Die Umkehrwalze bewirkt eine Permutation π, die eine echte Involution ist, d. h., kein Element wird auf sich selbst abgebildet. Das Steckerbrett bewirkt ebenfalls eine Involution η.

Die **Enigma-Substitution**, die Gesamtsubstitution im Zustand *z*, ist also

$$\rho_z = \eta^{-1} \circ \sigma_z^{-1} \circ \pi \circ \sigma_z \circ \eta$$

oder, ausführlich geschrieben, als **Enigma-Gleichung**:

$$c_i = \rho_z(a_i) = \eta^{-1}\, \tau^{z_1}\, \rho_1^{-1}\, \tau^{z_2-z_1}\, \rho_2^{-1}\, \tau^{z_3-z_2}\, \rho_3^{-1}\, \tau^{-z_3}\, \pi\, \tau^{z_3}\, \rho_3\, \tau^{z_2-z_3}\, \rho_2\, \tau^{z_1-z_2}\, \rho_1\, \tau^{-z_1}\, \eta\, (a_i).$$

Satz. *Die Enigma-Substitution ρ_z im Zustand z ist eine echte Involution.*

Beweis. Involution:

$$\rho_z^{-1} = \eta^{-1} \circ \sigma_z^{-1} \circ \pi^{-1} \circ \sigma_z \circ \eta = \rho_z\,,$$

da $\pi^{-1} = \pi$.

Echte Involution: Wäre $\rho_z(s) = s$ für einen Buchstaben $s \in \Sigma$, so wäre

$$\sigma_z\, \eta(s) = \sigma_z\, \eta\, \rho_z(s) = \pi\, \sigma_z\, \eta(s),$$

also $\pi(t) = t$ für $t = \sigma_z\eta(s) \in \Sigma$, im Widerspruch dazu, dass π eine echte Involution ist. ♦

Bemerkung. Dass η Involution ist, wurde dabei nicht benötigt. Es wurde wegen der Einfachheit der Realisierung so eingerichtet. Kryptographisch flexibler wären variable Verbindungsstecker zwischen dem Eingangsrotor und Tastatur/Lampenfeld.

Autor: Klaus Pommerening, 14. Dezember 1999; letzte Änderung: 7. Juli 2002

E-Mail an Pommerening@imsd.uni-mainz.de.