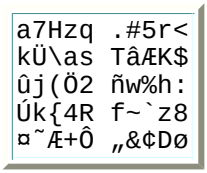
Kryptologie

Die Enigma - mathematisch betrachtet



Beschrieben wird hier die Enigma I (»Wehrmachts-Enigma«).

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 -- lässt man auch zu, dass weniger als 10 Stecker gesteckt werden, sind es sogar etwa $2.1 \cdot 10^{14}$ Möglichkeiten. Siehe dazu den Exkurs über Permutationen [PDF].
- 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 (in Bit ausgedrückt, was damals noch nicht üblich war). Davon gehen alleine 50 Bit auf das Konto des Steckerbretts.

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 $\lambda(x) = \delta_{x,m}$ (Kronecker-Symbol),

wobei m die Position des »Mitnehmers« (der Kerbe) ist. Die Periode ist also $26\cdot 25\cdot 26 = 16900$.

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 geringen Fehleranfälligkeit bei der Bedienung so eingerichtet. Kryptographisch flexibler wären variable Verbindungsstecker zwischen dem Eingangsrotor und Tastatur/Lampenfeld; aber davon bräuchte man auf jeden Fall 26.

Autor: Klaus Pommerening, 14. Dezember 1999; letzte Änderung: 13. Januar 2008.