Die kommerzielle Enigma

Die Enigma-Typen C und D, also die mit der Umkehrwalze, waren frei auf dem Markt erhältlich und konnten somit in ihrer Funktionsweise ausführlich analysiert werden.

> Die Enigma D wurde im spanischen Bürgerkrieg von allen Parteien eingesetzt und von allen Großmächten gebrochen.

Die kommerzielle Enigma hatte kein Steckerbrett - die Substitution reduziert sich somit auf

$$c_i = \sigma_z^{-1}\, \pi\, \sigma_z\, (a_i),$$

wobei σ_z die durch die drei Walzen bewirkte Substitution im Zustand $z = (z_1, z_2, z_3)$ ist.

Kryptoanalytischer Ansatz

Suche nach Isomorphen

In einem Abschnitt, wo sich nur der Rotor 1 bewegt, bewirken die beiden inneren Rotoren zusammen mit der Umkehrwalze eine konstante Involution $\pi^{\sim}$. In diesem Abschnitt bestehen bei bekanntem Klartext dann Gleichungen

$$\begin{aligned} c_1 &= [\rho_1^{(z_1)}]^{-1}\, \pi^{\sim}\, \rho_1^{(z_1)}\, (a_1), \\ c_2 &= [\rho_1^{(z_1+1)}]^{-1}\, \pi^{\sim}\, \rho_1^{(z_1+1)}\, (a_2), \\ &\dots \\ c_m &= [\rho_1^{(z_1+m-1)}]^{-1}\, \pi^{\sim}\, \rho_1^{(z_1+m-1)}\, (a_m). \end{aligned}$$

Also ist für $i = 1, \dots, m$

$$c_i' = \rho_1^{(z_1+i-1)}\, (c_i) = \pi^{\sim}\, \rho_1^{(z_1+i-1)}\, (a_i) = \pi^{\sim}\, (a_i')$$

monoalphabetisches Bild von $a_i' = \rho_1^{(z_1+i-1)}\, (a_i)$ unter der Involution $\pi^{\sim}$.

Also ist durch Mustervergleich beim Durchprobieren aller Rotoren und Ausgangsstellungen der schnelle Rotor und sein Zustand identifizierbar. Dazu sind auf der rechten Seite - der Bestimmung von a_i' aus a_i - alle drei Rotoren mit ihren jeweils 26 möglichen Startstellungen durchzuprobieren. Auf der linken Seite wird c_i' mit dem gleichen Rotor in der gleichen Stellung aus c_i gebildet. Das macht insgesamt 3×26 = 78 zu testende Konstellationen, die jeweils auf übereinstimmendes Muster getestet werden. In der Regel wird es mehrere, aber nur wenige passende Lösungen geben.

Für jede der herausgefischten möglichen Lösungen wird auch noch geprüft, ob der Übergang von den a_i' zu den c_i' für $i = 1, ..., m$ damit verträglich ist, dass $\pi^{\sim}$ eine feste Involution ist -- d. h., ob es widersprechende Zuordnungen $c_i' = \pi^{\sim}(a_i')$ und $c_j'' = \pi^{\sim}(a_j'')$ mit $c_i' = a_j''$ und $c_j'' = a_i'$ gibt; dabei scheiden weitere Kandidaten aus, und für $\pi^{\sim}$ sind dann schon jeweils einige der Zweierzyklen bestimmt, so dass man längst nicht mehr alle $26^2 = 576$ Möglichkeiten für die Stellung der beiden inneren Rotoren ausprobieren muss. Als Hilfsmittel dient jeweils eine vorausberechnete vollständige Tabelle der Länge 576 für die 6 verschiedenen Kombinationen dieser beiden Rotoren, die zu allen Zuständen die Zerlegung von $\pi^{\sim}$ in Zweierzykel enthält.

Die Lage von bekanntem Klartext kann man, wenn sie nicht von vornherein feststeht, durch negative Mustersuche einschränken.

Folgerung

Die Einführung der Umkehrwalze sollte die Sicherheit der Enigma dadurch drastisch erhöhen, dass die Zahl der Rotor-Durchquerungen verdoppelt wurde. Dies hat sich somit als *illusorische Komplikation* herausgestellt. Der obige Angriff reduziert die Kryptoanalyse auf die Exhaustion der Lage und Stellung von nur drei Rotoren, und selbst die wird noch stark reduziert.

Um diesen Angriff zu verhindern, wurde beim Übergang zur Wehrmachts-Enigma das Steckerbrett eingeführt.

Autor: Klaus Pommerening, 13. Februar 2000; letzte Änderung: 13. Januar 2008.