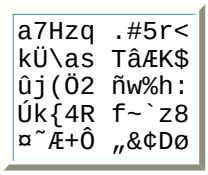
Kryptologie

Kryptoanalyse der Enigma I nach REJEWSKI



Spruchschlüssel-Analyse (Fortsetzung 2)

REJEWSKIs Katalog

Die Permutationen $\tau_1 = \rho_4\rho_1$, $\tau_2 = \rho_5\rho_2$ und $\tau_3 = \rho_6\rho_3$ sind im Beispiel schon vollständig bestimmt; ihre Zykel-Darstellung ist:

```
τ1: (A) (BC) (DVPFKXGZYO) (EIJMUNQLHT) (RW) (S)
τ2: (AXT) (BLFQVEOUM) (CGY) (D) (HJPSWIZRN) (K)
τ3: (ABVIKTJGFCQNY) (DUZREHLXWPSMO)
```

Wir nehmen jetzt an, dass die Walzen-Verdrahtung bekannt ist, und fahren mit der Analyse fort.

Die Zykel-Typen, beschrieben durch Partitionen von 26, unserer drei Permutationen τ_1, τ_2 und τ_3 sind

```
[10 10 2 2 1 1], [9 9 3 3 1 1], [13 13].
```

Die Frage ist nun, wie weit dieses Tripel von Partitionen für die Grundstellung charakteristisch ist. Da die Steckerverbindungen hierfür keine Rolle spielen, wird die Grundstellung charakterisiert durch eine Permutation der drei Walzen, also ein Element der Permutationsgruppe $\mathbf{S}_3$, sowie je einer Anfangstellung jeder Walze, die sich als Element der zyklischen Gruppe $\mathbf{Z}/26\mathbf{Z}$ beschreiben lässt, insgesamt haben wir - unter Vernachlässigung der Ringstellung - die Menge $\mathbf{S}_3 \times (\mathbf{Z}/26\mathbf{Z})^3$ von Grundstellungen. Auf der anderen Seite haben wir die Menge $\mathbf{P}_{13}$ aller 101 Partitionen der Zahl 13 (entspricht der Menge der Partitionen von 26 in paarweise gleiche Teile) und eine Abbildung

$$\mathbf{S}_3 \times (\mathbf{Z}/26\mathbf{Z})^3 \to (\mathbf{P}_{13})^3$$

Ideal wäre es, wenn diese Abbildung injektiv wäre; das wäre aufgrund der Kardinalitäten, nämlich 105456 für die Grundstellungen, $101^3 = 1030301$ für die Partitionen, auf den ersten Blick möglich.

Um die Abbildung vollständig zu beschreiben, ließ REJEWSKI einen einfachen Enigma-Simulator, genannt Zyklometer, bauen, der in etwa einem Jahr alle Grundstellungen durchlief. Das Ergebnis, genannt REJEWSKIs Katalog, existiert nicht mehr, wurde aber unlängst rekonstruiert:

> Alex Kuhl: Rejewski's Catalog. Cryptologia 31 (2007), 326-331.

Es stellte sich heraus, dass die Abbildung nicht injektiv ist, aber viele Partitionstripel nur ein Urbild, die meisten nur wenige Urbilder haben. Allerdings gibt es auch einige wenige Muster, die sehr häufig sind. Insgesamt kommen 21230 verschiedene Muster vor. Die Anzahlen selten (bis zehnmal) vorkommender Muster sind

Vorkommen:	1	2	3	4	5	6	7	8	9	10
Anzahl:	11466	3381	1658	958	660	456	343	265	234	183

Insgesamt kommen also 19604 Muster höchstens zehnmal vor, das sind über 92%. Andererseits sind einige Muster auch recht häufig; die zehn häufigsten sind

Muster			**Häufigkeit**
[13 13]	[13 13]	[13 13]	1771
[12 12 1 1]	[13 13]	[13 13]	898
[13 13]	[13 13]	[12 12 1 1]	866
[13 13]	[12 12 1 1]	[13 13]	854
[11 11 2 2]	[13 13]	[13 13]	509
[13 13]	[12 12 1 1]	[12 12 1 1]	494
[13 13]	[13 13]	[11 11 2 2]	480
[12 12 1 1]	[13 13]	[12 12 1 1]	479
[13 13]	[11 11 2 2]	[13 13]	469
[12 12 1 1]	[12 12 1 1]	[13 13]	466

Mit Hilfe dieses Katalogs konnten die polnischen Kryptoanalytiker die korrekte Grundstellung normalerweise in höchstens zwanzig Minuten bestimmen. Was sie in den Ausnahmesituationen machten, wo das Ergebnis zu vieldeutig war, ist nicht bekannt; die Informationen, die man in der Fortsetzung 1 der Analyse gewinnen kann, helfen hier aber sicher auch weiter. Gehen wir also davon aus, dass die Ermittlung der Grundstellung nach dieser Methode bei mindestens 92% der Muster erfolgreich war; das dürfte etwa 50% der Fälle entsprechen.

Jetzt kommt aber noch der Effekt der Ringstellung hinzu. Diese bewirkt ja eine Variation in der Walzen-Weiterschaltung, da die Mitnehmer-Kerbe fest mit dem Alphabetring verbunden ist. Nun, was kann passieren? Solange sich nur die erste Walze dreht, haben wir eine der Situationen im Katalog - unter der Annahme, dass er dafür gemacht ist. Gestört wird die Analyse, wenn sich die zweite Walze zwischen den Buchstaben 1 bis 6 dreht; dafür gibt es 5 Möglichkeiten von insgesamt 26 Ringstellungen der ersten Walze. Die Wahrscheinlichkeit dieser Störung ist also 5/26, also etwa 19%. Das verringert die gesamte Erfolgswahrscheinlichkeit von 50% auf etwa 40%. Um das zu abzufangen, bräuchte man noch 5 weitere Kataloge, die die jeweilige Weiterschaltung der zweiten Walze berücksichtigen.

Allerdings sind die Möglichkeiten, aus den gesammelten Nachrichtenanfängen Folgerungen zu ziehen, noch nicht erschöpft. Es ist sogar so, dass die Störung durch die Bewegung der zweiten Walze Auskunft über die Ringstellung gibt. Darauf wollen wir hier aber nicht näher eingehen, sondern einfach annehmen, dass Walzenlage und Grundeinstellung bestimmt sind.

Der einfachste, oft funktionierende Ansatz, die noch fehlenden Steckerverbindungen zu finden, beruht darauf, dass zunächst ja maximal sechs Buchstabenpaare vertauscht wurden. Wird also mit der Enigma ganz ohne Steckverbindungen entschlüsselt, so scheint genügend viel an Klartext durch, dass man diesen und somit auch die Steckersubstitution rekonstruieren kann.

Autor: Klaus Pommerening, 6. Januar 2008; letzte Änderung: 13. Januar 2008.