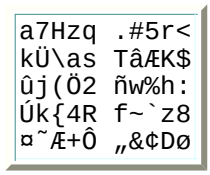
Kryptologie

Kryptoanalyse der Enigma I nach REJEWSKI

Spruchschlüssel-Analyse (Fortsetzung 1)



Bestimmung der Enigma-Substitutionen aus der Tages-Charakteristik

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:

τ_1: `(A) (S) (BC) (RW) (DVPFKXGZYO) (EIJMUNQLHT)`
τ_2: `(D) (K) (AXT) (CGY) (BLFQVEOUM) (HJPSWIZRN)`
τ_3: `(ABVIKTJGFCQNY) (DUZREHLXWPSMO)`

Wir versuchen jetzt, die ersten sechs Enigma-Substitutionen der Grundstellung, ρ_1 bis ρ_6, aus diesen Produkten $\tau_1 = \rho_4\rho_1$, $\tau_2 = \rho_5\rho_2$ und $\tau_3 = \rho_6\rho_3$ zu bestimmen. Die versuchsweise Anordnung dazu [siehe den Exkurs über Permutationen: PDF] ist:

```
(A) (BC) (DVPFKXGZYO)
(S) (WR) (THLQNUMJIE)

(D) (AXT) (BLFQVEOUM)
(K) (YGC) (NRZIWSPJH)

(ABVIKTJGFCQNY)
(OMSPWXLHERZUD)
```

Daraus lässt sich bereits schließen, dass ρ_1 und ρ_4 jeweils den Zweierzykel `(AS)` und ρ_2 und ρ_5 jeweils den Zweierzykel `(DK)` haben. Aber schon bei den Zweierzykeln von τ_1 gibt es keine eindeutige Lösung: Es kann ρ_1 die Zykeln `(BW)(CR)` und ρ_4 die Zykeln `(BR)(CW)` haben oder umgekehrt.

Nimmt man nun mit REJEWSKI an, dass `aaa` der beliebteste Spruchschlüssel ist -- im Misserfolgsfall würde man andere Stereotype ausprobieren --, so könnte dieser dem fünffach aufgefangenen Nachrichtenanfang `SYX SCW` entsprechen. Das würde bedeuten, dass folgende Zykel vorkommen:

`(AS)` in ρ_1, `(AS)` in ρ_4,
`(AY)` in ρ_2, `(AC)` in ρ_5,
`(AX)` in ρ_3, `(AW)` in ρ_6.

Für ρ_1 und ρ_4 ist das keine neue Erkenntnis. Für τ_2 bedeutet es, dass die Anordnung der Dreierzykel schon die richtige ist, und weitere Zweierzykel abgelesen werden können:

`(AY)(XG)(TC)` in ρ_2, `(AC)(GT)(XY)` in ρ_5.

Bei τ_3 haben wir die Anordnung

```
(ABVIKTJGFCQNY)
(XLHERZUDOMSPW)
```

die schon die eindeutige Lösung

ρ_3 = (AX)(BL)(CM)(DG)(EI)(FO)(HV)(JU)(KR)(NP)(QS)(TZ)(WY),
ρ_6 = (AW)(BX)(CO)(DF)(EK)(GU)(HI)(JZ)(LV)(MQ)(NS)(PY)(RT),

ablesen lässt.

Betrachten wir nun andere Nachrichtenanfänge, etwa den ersten: `AUQ AMN`. Der zugehörige Klartext muss

```
s?s s?s
```

sein. Das lässt den stereotypen Spruchschlüssel `sss` vermuten. Damit hätte ρ_2 den Zykel `(SU)` und ρ_5 den Zykel `(MS)`. Damit ist auch die richtige Überlagerung der Neunerzykel von τ_2 gefunden:

```
(D) (AXT) (BLFQVEOUM)
(K) (YGC) (JHNRZIWSP)
```

und damit sind auch

ρ_2 = (AY)(BJ)(CT)(DK)(EI)(FN)(GX)(HL)(MP)(OW)(QR)(SU)(VZ),
ρ_5 = (AC)(BP)(DK)(EZ)(FH)(GT)(IO)(JL)(MS)(NQ)(RV)(UW)(XY)

vollständig bestimmt.

Die vierfach auftretende Gruppe `RJL WPX` entspricht jetzt dem Klartext

```
?bb ?bb,
```

deutet also wieder sehr überzeugend auf den stereotypen Spruchschlüssel `bbb` hin. Dann hat ρ_1 den Zykel `(BR)` - und damit auch `(CW)` - und ρ_4 den Zykel `(BW)` und somit auch `(CR)`.

Nun ist nur noch die Anordnung der beiden Zehnerzykel von τ_1 zu bestimmen. Das geht z. B. mit der Gruppe `LDR HDE`: Sie wird bis jetzt zu

```
?kk ?kk
```

entschlüsselt. Also vermuten wir hier mit schon an Sicherheit grenzender Zuversicht, dass der Spruchschlüssel `kkk` war. Das ergibt für ρ_1 den Zykel `(KL)` und damit die Überlagerung

```
(A) (BC) (DVPFKXGZYO)
(S) (RW) (IETHLQNUMJ)
```

der Zykel von τ_1. Damit sind auch ρ_1 und ρ_4 bestimmt:

ρ_1 = (AS)(BR)(CW)(DI)(EV)(FH)(GN)(JO)(KL)(MY)(PT)(QX)(UZ),
ρ_4 = (AS)(BW)(CR)(DJ)(EP)(FT)(GQ)(HK)(IV)(LX)(MO)(NZ)(UY).

Damit lassen sich jetzt insbesondere alle Spruchschlüssel zum momentanen Grundschlüssel entziffern. Allerdings ist der Grundschlüssel selbst damit noch nicht bestimmt, und die Entzifferung der eigentlichen Nachrichten auch noch nicht möglich - vor allem, da die Ringstellung - und damit

die eigentliche Stellung der Walzen - noch unbekannt ist.

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