Kryptologie

Rotor-Maschinen: Beispiele für die Steuerlogik

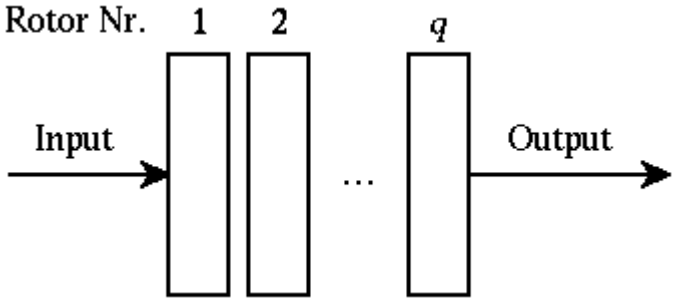
```
a7Hzq .#5r<
kÜ\as TâÆK$
ûj(Ö2 ñw%h:
Úk{4R f~`z8
¤˜Æ+Ô „&¢Dø
```

Hier werden fünf Beispiele für die Steuerlogik von Rotor-Maschinen behandelt - zwei idealisierte, die in der Praxis meist komplizierter konstruiert wurden: das Zählwerk und der Stangenkorb, zwei realistische: die ungleichen Antriebszahnräder und die pseudozufällige Weiterschaltung, und eine historische: die Hebern-Maschine. Die Steuerlogik der Enigma wird später behandelt.

Die Erkenntnis, dass die Steuerlogik für die Sicherheit einer Rotor-Maschine von entscheidender Bedeutung ist, hatte wohl FRIEDMAN als erster, nachdem er die HEBERN-Maschine gebrochen hatte. Er entwickelte dann selbst die »ultimative« Rotor-Maschine SIGABA.

Beispiel 1: Das Zählwerk

Hier werden die Rotoren wie bei einem Stromzähler oder Tachometer weitergeschaltet: Jeder Rotor hat einen »Mitnehmer«, z. B. einen Nippel, der nach einer vollen Umdrehung den Nachbar-Rotor um eine Stelle weiterbewegt. Die Rotoren sollen dabei wie folgt angeordnet sein:



Die Zustandsfolge sieht allgemein so aus:

Zustand	Rotorstellungen					Substitution
$z^{(0)}$	z_{01}	z_{02}	...	...	z_{0q}	$c_0 = \sigma(a_0)$
$z^{(1)}$	z_{11}	z_{12}	...	...	z_{1q}	$c_1 = \sigma(a_1)$
$z^{(2)}$	z_{21}	z_{22}	...	...	z_{2q}	$c_2 = \sigma(a_2)$
:	:	:			:	:
$z^{(i)}$	z_{i1}	z_{i2}	...	...	z_{iq}	$c_i = \sigma(a_i)$
:	:	:			:	:

Der *i*-te Zustand wird durch folgende Gleichung beschrieben, wobei das Alphabet Σ mit **Z**/*n***Z** identifiziert wird und modulo *n* addiert wird:

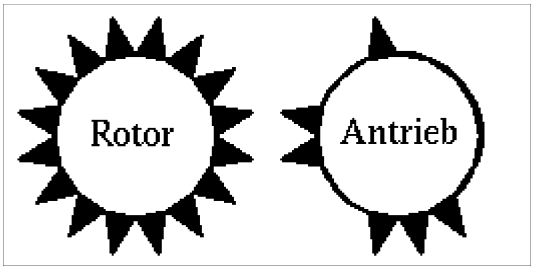
$$z^{(i)} = \left(z_{01} + \left[\frac{i}{n^{q-1}} \right], \cdots, z_{0j} + \left[\frac{i}{n^{q-j}} \right], \cdots, z_{0q} + i \right)$$

Bemerkungen

1. Der *q*-te, rechte, Rotor ist in diesem Beispiel ein »schneller« Rotor: Er dreht sich bei jedem Schritt.
2. Dagegen ist der erste, linke, Rotor ein »langsamer« Rotor. Er dreht sich fast nie - nur alle n^{q-1} Schritte, also überhaupt nur bei sehr langen Nachrichten.
3. Die Zählerfortschaltung kann natürlich genauso leicht auch umgekehrt realisiert werden, so dass der linke, der Input-Rotor, der schnelle und der rechte, der Output-Rotor, der langsame ist.
4. Einer andere, in der Praxis auch verwendete Methode ist, den *j*-ten Rotor nicht erst nach n^{q-j} Schritten weiterzubewegen, sondern schon wenn der Zustand $z_{i,j-1} = n$ erreicht wird. Das ist je nach Anfangszustand viel früher und entspricht mehr der intuitiven Vorstellung von einem Zähler.
5. In jedem Fall hat die Zustandsfolge die Periode n^q.

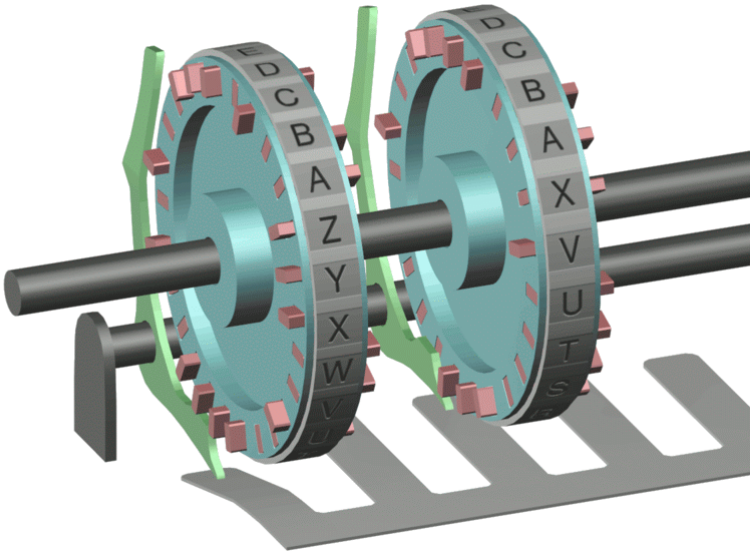
Beispiel 2: Zahnlücken

Eine unregelmäßige Fortschaltung, bei der es aber keine langen Pausen für einzelne Rotoren gibt, kann man erreichen, indem man jeden Rotor durch ein Zahnrad antreibt, das unterschiedliche Lücken hat:



Die ersten Modelle der Enigma (Modell A und B) hatten solche Antriebszahnräder (die außerdem auch noch verschiedene Umfänge hatten).

Eine übliche Realisierung dieses Antriebs ist das **Bolzenrad** (Stiftwalze, Sprossenrad, Schlüsselrad, »pin wheel«) mit einstellbaren Bolzen oder Schaltstiften. Hier werden Bolzen nach links oder rechts geschoben; eine von beiden Positionen ist die aktive, bei der das Nachbarrad zum Weiterdrehen veranlasst wird, die andere Position ist die passive. Eine Illustration von der HAGELIN-Maschine M-209:



wo die Bolzen allerdings nicht ein Zahnrad weiterbewegen, sondern einen Hebel auslenken. [Die M-209 ist auch ein Schlüssel-Erzeuger und keine eigentliche Rotor-Maschine.]

Eine andere Realisierung dieses Prinzips, der »Stangenkorb« wurde von HAGELIN erfunden und ist ebenfalls bei der M-209 im geöffneten Zustand deutlich zu erkennen. Anstelle eines Zahnrades wird ein Zylinder aus Stangen verwendet, der über die ganze Breite des Walzenkorbs reicht und einstellbare Nippel (»lugs«) hat. Diese bewirken, wenn ein aktiver Bolzen eines Schlüsselrads den Hebel auslöst, eine Verschiebung der jeweiligen Stange nach links. In jeder Phase sind also einige Stangen links herausgeschoben und einige nicht, so dass wieder eine Art Zahnlückenrad entsteht.

Ein einzelnes Antriebsrad kann man durch einen binären Vektor charakterisieren: 1 bedeutet Zahn, 0 bedeutet Zahnlücke:

$$u_{(j)} = (u_{j0},\ldots,u_{j,t-1}) \in \mathbf{F}_2{}^t \quad \text{für } j = 1, \ldots, q;$$

dabei ist t der Umfang des Antriebsrads (muss nicht notwendig = n sein); wir können ihn also insgesamt durch eine Matrix

$$u = \begin{pmatrix} u_{10} & \cdots & u_{1,t-1} \\ \vdots & \ddots & \vdots \\ u_{q0} & \cdots & u_{q,t-1} \end{pmatrix} \in \mathbf{M}_{q,t}(\mathbf{F}_2)$$

beschreiben. Die Spaltenvektoren

$$u^{(i)} = (u_{1i},\ldots,u_{q,i}) \in \mathbf{F}_2{}^q \quad \text{für } i = 0, \ldots, t\text{-}1$$

werden periodisch fortgezählt und ergeben so eine Folge der Periode t.

Die Zustandsänderung wird damit so beschrieben: Im Schritt i bewegt sich der j-te Rotor

- nicht, wenn $u_{ji} = 0$,
- um eine Position, wenn $u_{ji} = 1$.

Die Zustandsänderung geht also nach der Formel

$$z^{(i+1)} = z^{(i)} + u^{(i)},$$

wobei in $(\mathbf{Z}/n\mathbf{Z})^q$ addiert wird.

Natürlich kann man das Antriebsrad mit Zahnlücken auch durch ein Antriebsrad mit allen Zähnen ersetzen, das aber seinerseits durch eine Steuerlogik jeweils um eine oder null Stellen weitergedreht wird.

Beispiel 3: Die ungleichen Antriebszahnräder

Hier hat jeder Rotor ein eigenes Antriebszahnrad; diese sitzen auf einer gemeinsamen Achse und machen bei jedem Buchstaben eine volle Drehung. Rotor 1 wird also um n_1 Stellungen weitergedreht, wenn n_1 die Zahl der Zähne seines Antriebsrades ist. Analog für die anderen Rotoren. Die Periode des Zustandes ist daher das kgV(n_1, ...,n_q). Besonders günstig sind also paarweise teilerfremde Zahnanzahlen, z. B. die Folge 17, 19, 21, 23, 25, 29, 31, 32.

Dieses Prinzip wurde - mit Zahnlückenrädern - bei den ersten Versionen der Enigma mit den Zahlen 11, 15, 17, 19 verwendet.

Beispiel 4: Die pseudozufällige Weiterschaltung

Hierbei wird die Folge der Weiterschaltungen für jeden Rotor nach einem Pseudozufallszahlen-Algorithmus bestimmt; in einer Computersimulation ist das leicht, für eine elektromechanische Rotormaschine kann man etwa zusätzlich einen Schlüsselerzeuger wie die späteren HAGELIN-Maschinen zur Steuerung des Antriebs verwenden. Nach diesem Prinzip soll die amerikanische Super-Rotormaschine SIGABA gearbeitet haben.

Beispiel 5: Die Hebern-Maschine

Die HEBERN-Maschine hat $q = 5$ Rotoren und verwendet das Standard-Alphabet mit $n = 26$. Die Steuerlogik ist ein Zählwerk, wobei allerdings nicht der benachbarte Rotor, sondern über eine etwas kompliziertere Mechanik ein anderer weitergeschaltet wird, und zwar genauer:

- Die Rotoren 2 und 4 drehen sich gar nicht (»Statoren«).
- Rotor 5 dreht sich bei jedem Schritt um 1 weiter, ist also ein schneller Rotor.
- Rotor 1 wird bei jeder vollen Umdrehung von Rotor 5 um eine Position mitgenommen, ist also ein mittelschneller Rotor.
- Rotor 3 wird bei jeder vollen Umdrehung von Rotor 1 um eine Position mitgenommen, ist also ein langsamer Rotor.

Die Zustandsänderung folgt also der Gleichung (im wesentlichen - siehe »Besonderheiten«)

$$g(z_1, z_2, z_3, z_4, z_5) = (z_1+\lambda(z_5), z_2, z_3+\lambda(z_1)\lambda(z_5), z_4, z_5+1)$$

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

Die Periode ist also $26^3 = 17576$.

Besonderheiten

- Der Verzicht auf die Drehung der Rotoren 2 und 4 ist kein Verlust an Sicherheit, wenn sie nach dem Zählwerk-Prinzip sowieso erst nach $26^3 = 17576$ bzw. 26^4 Schritten bewegt würden. Solch lange Nachrichten kommen in der Praxis der damaligen Zeit nicht vor.
- Das Weiterschalten von Rotor 1 bzw. 3 geschieht immer dann, wenn Rotor 5 bzw. 1 von der Stellung »N« weiterschaltet. Die korrekte Form der Gleichung für die Zustandsänderung bleibt dem Leser überlassen [**Übungsaufgabe**].
- Die Verdrahtung von der Tastatur zum Rotor 1 einerseits und vom Rotor 5 zu den Glühlämpchen andererseits ist unregelmäßig und definiert somit jeweils eine feste zusätzliche Substitution (die allerdings als dem Gegner bekannt angenommen werden muss).
- Zum Zwecke der Entschlüsselung wird ein Schalter »Direct/Reverse« umgelegt, der Input- und Output-Kontakte vertauscht.
- Die Rotoren der HEBERN-Maschine sind äußerlich symmetrisch, können also auch umgekehrt eingesetzt werden. Dadurch vergrößert sich die Zahl der Möglichkeiten, also der Primärschlüssel-Raum deutlich (um den Faktor 2^5).

Autor: Klaus Pommerening, 1. Januar 2000; letzte Änderung: 27. Januar 2008.