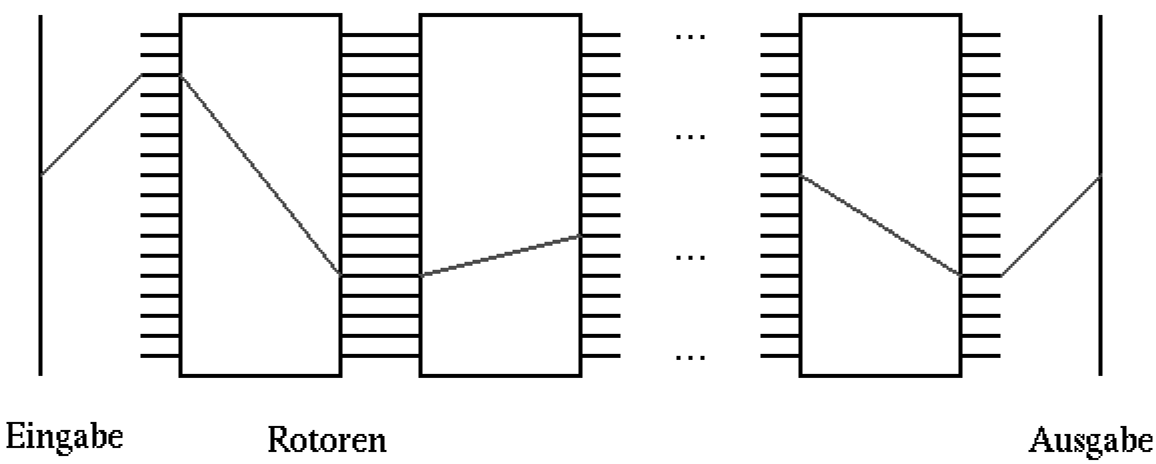
Kryptologie

Rotor-Maschinen

Allgemeine Beschreibung

Rotormaschinen sind elektromechanische Geräte, die aus mehreren, hintereinandergeschalteten Rotoren (oder »Walzen«) bestehen.

Eine Vorstellung vom Stromlauf durch eine solche Maschine vermittelt das Bild



oder die Seite Rotor Machine Basics von John Savard.

Nach jedem eingegebenen Buchstaben drehen sich die Rotoren unterschiedlich weiter, manche um einen Kontakt, manche vielleicht um mehrere, manche gar nicht.

Die kryptographische Sicherheit der Rotormaschinen beruht - neben der Anzahl der möglichen Rotoren und der Vielzahl der Einstellmöglichkeiten (also der Größe des Schlüsselraums) - *auf der Komplexität des Weiterschaltmechanismus der Rotoren.*

Bedienung: Eine Taste auf der Schreibmaschinen-Tastatur des Verschlüsselungsgeräts wird gedrückt (= Eingabe eines Klartextbuchstabens). Ein Lämpchen mit einem Buchstaben leuchtet auf (= Ausgabe des zugehörigen Geheimtextbuchstabens). [Aufwendigere Version: Ein Buchstabe wird gedruckt.] Gleichzeitig (etwa beim Loslassen der Taste) drehen sich die Rotoren.

Das geheimnisvoll unregelmäßig drehendende Räderwerk macht diese Art von Geräten attraktiv - so stellt sich der »kleine Moritz« eine Verschlüsselungsmaschine vor.

Rotormaschinen sind der Stand der Verschlüsselungstechnik in der Periode etwa 1920 - 1960.

Mathematische Beschreibung

Diese abstrakte Beschreibung soll das Funktionsprinzip klar machen. Sie deckt konkrete, historische Rotor-Maschinen nicht notwendig in allen Details ab, da in diese oft individuelle Komplikationen eingebaut wurden.

Das Alphabet Σ wird wie üblich mit $\mathbf{Z}/n\mathbf{Z}$, den ganzen Zahlen modulo n, identifiziert. Dann kann man eine Rotor-Maschine durch folgende Parameter charakterisieren:

- Eine Menge $R \subseteq \mathbf{S}(\Sigma)$ von $p = \#R$ Rotoren (der »**Walzenkorb**«), jeder davon durch ein Primäralphabet, also eine Permutation $\rho_i \in \mathbf{S}(\Sigma)$ beschrieben, die der inneren Verdrahtung des Rotors entspricht.

- Eine Auswahl $\rho = (\rho_1, ..., \rho_q) \in \mathbf{S}(\Sigma)^q$ mit $\{\rho_1, ..., \rho_q\} \subseteq R$ von q der Rotoren (»**Walzenlage**«), wofür es $p \cdot (p\text{-}1)\cdots(p\text{-}q\text{+}1)$ Möglichkeiten gibt (falls alle Rotoren verschieden verdrahtet sind). Diese Auswahl dient als »Primärschlüssel«, der für mehrere Nachrichten, z. B. einen Tag lang, ungeändert bleibt.
[Ganz formal ist die Auswahl eine injektive Abbildung des ganzzahligen Intervalls $[1..q]$ nach R.]

- Einen Zustandsvektor $z = (z_1,...,z_q) \in \Sigma^q$, der die aktuelle **Rotorstellung** beschreibt.
Als »Sekundärschlüssel« dient die Anfangsstellung $z^{(0)}$, die oft, etwa für jede Nachricht, neu gewählt wird (»Spruchschlüssel«); dafür gibt es n^q Möglichkeiten.

- Eine Zustandsänderungsfunktion

  $$g\colon \mathbf{N} \times \Sigma^q \to \Sigma^q,$$

  die den Zustand $z^{(i)}$, in dem der i-te Buchstabe verschlüsselt wird, in den Zustand

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

  überführt. (Weiterschalt-Mechanismus oder **Steuerlogik**, realisiert z. B. durch mehr oder weniger komplizierte Zahnradgetriebe.)

- Die **aktuelle Substitution** im Zustand z:

  $$\sigma_z = \rho_q^{(z_q)} \circ \ldots \circ \rho_1^{(z_1)} \in \mathbf{S}(\Sigma) \quad \text{mit } \rho_j^{(z_j)} = \tau^{z_j} \circ \rho_j \circ \tau^{-z_j}.$$

  Der Klartext $\in \Sigma^r$ wird also nach der Vorschrift

  $$c_i = \sigma_{z^{(i)}}(a_i)$$

  verschlüsselt.

Ideal wäre es, wenn die Abbildung

$$\Sigma^q \to \mathbf{S}(\Sigma), \quad z \to \sigma_z,$$

injektiv wäre. Darüber gibt es allerdings keine brauchbaren allgemeinen Aussagen.

Ver- und Entschlüsselung

Ausführlich geschrieben sieht die Verschlüsselungsfunktion so aus:

$$c_i = \tau^{z_q^{(i)}} \circ \rho_q \circ \tau^{z_{q-1}^{(i)}-z_q^{(i)}} \circ \ldots \circ \tau^{z_1^{(i)}-z_2^{(i)}} \circ \rho_1 \circ \tau^{-z_1^{(i)}} (a_i)$$

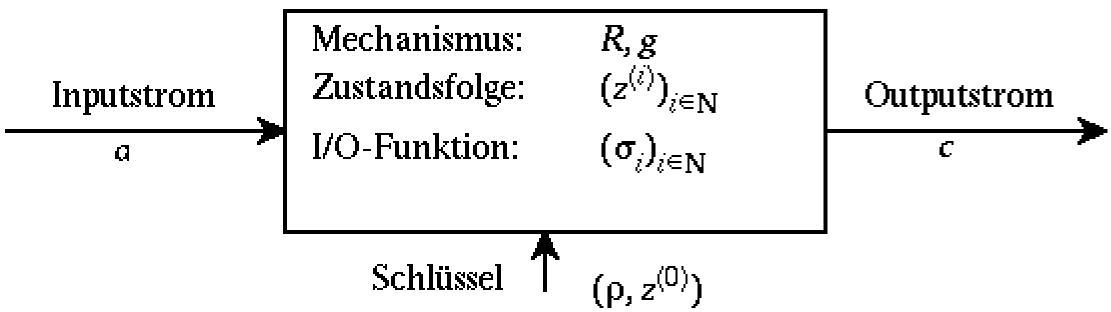
und die entsprechende Entschlüsselungsfunktion so:

$$a_i = \tau^{z_1^{(i)}} \circ \rho_1^{-1} \circ \tau^{z_2^{(i)}-z_1^{(i)}} \circ \ldots \circ \tau^{z_q^{(i)}-z_{q-1}^{(i)}} \circ \rho_q^{-1} \circ \tau^{-z_q^{(i)}} (c_i)$$

Die Entschlüsselung geschieht selbstverständlich einfach dadurch, daß der Strom in umgekehrter Richtung durch die Rotoren geschickt wird, d. h., Tastatur und Lampensatz müssen vertauscht angestöpselt werden; die Reihenfolge der Zustände ist die gleiche wie bei der Verschlüsselung.

Beschreibung als endlicher Automat

Abstrakt wird eine Rotor-Maschine so beschrieben:



Einschub: Perioden von Zustandsänderungen

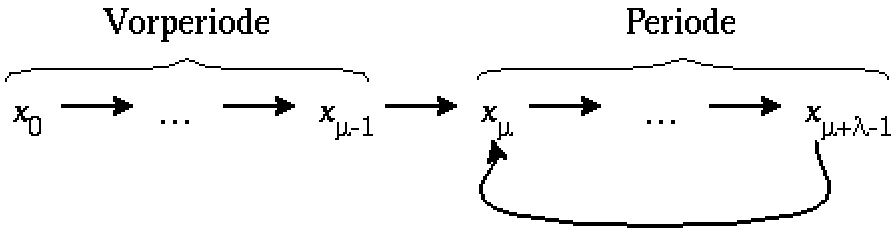
Meist ist die Zustandsänderungsfunktion vom Schritt i unabhängig. D. h., wir können einfacher annehmen

$$g: \Sigma^q \to \Sigma^q.$$

Etwas allgemeiner haben wir also eine endliche Menge M (statt Σ^q) mit $m = \#M$ (statt n^q) und eine Abbildung

$$g: M \to M.$$

Zu jedem Startwert (»Anfangszustand«) $x_0 \in M$ wird durch die einstufige Rekursionsformel $x_i = g(x_{i-1})$ für $i \geq 1$ eine Folge in M erzeugt. Diese mündet nach einer Vorperiode der Länge μ in eine periodische Folge der Länge λ:



Wegen der Endlichkeit von M gibt es nämlich kleinste Zahlen $\mu \geq 0$ und $\lambda \geq 1$ mit $x_{\mu+\lambda} = x_\mu$.

Dann gilt auch

$$x_{i+\lambda} = x_i \quad \text{für } i \geq \mu.$$

Natürlich ist stets $0 \leq \mu \leq m - 1$, $1 \leq \lambda \leq m$, $\lambda + \mu \leq m$.

Der Schlüsselraum

Ein Schlüssel besteht nach der obigen Beschreibung aus

- einer Auswahl der Rotoren,
- einem Anfangszustand.

Die Größe des Schlüsselraums ist also

$$\#K = n^q \cdot p!/(p-q)!.$$

In einem typischen Fall (Hebern-Maschine) ist $p = q = 5$, $n = 26$, $\#K = 120 \cdot 26^5 = 712\,882\,560$, und die effektive Schlüssellänge $d(F) \approx 29.4$. Das war 1920 groß genug, ist gegen einen computerbesitzenden Angreifer aber völlig ungenügend.

Beispiele für die Steuerlogik

Autor: Klaus Pommerening, 31. Dezember 1999; letzte Änderung: 12. Juni 2002

E-Mail an `Pommerening@imsd.uni-mainz.de`.