

# TECHNIKGESCHICHTE DIE VORFAHREN DER ENIGMA UND DES COMPUTERS

**SERIE: GOTTFRIED WILHELM LEIBNIZ** Der Universalgelehrte hat seine mechanischen Wunderwerke nie voll funktionsfähig erlebt. Seit wir sie rekonstruiert haben, wissen wir: Leibniz war seiner Zeit um Jahrhunderte voraus.



**Klaus Badur** hat eine Lehre als Maschinenschlosser und ein Ingenieurstudium in Hannover durchlaufen. Nach Tätigkeiten in der Industrie als Konstrukteur und Projekt ingenieur war er ab 1988 Geschäftsführer einer international tätigen Entwicklungsfirma für Mess- und Prüfmaschinen im Automobilbau. Seitdem er 2013 in Ruhestand ging, betreibt er private Forschung zu historischen mechanischen Rechenmaschinen, einerseits durch Studium der Werke Leibnizens, andererseits durch Restaurierung und Nachbau auch anderer Geräte.

► [spektrum.de/artikel/1382049](http://spektrum.de/artikel/1382049)

Ein wahrhaft monumentales Werk hat Gottfried Wilhelm Leibniz uns hinterlassen. Schon die schiere Menge des Materials ist beeindruckend: Die annähernd 100 000 Blatt Papier, die er im Lauf seines Lebens beschrieben hat, füllen ein Volumen von ungefähr zwei Kubikmetern. Und die hochphilosophischen Gedanken über die beste aller Welten (Teil 1 dieser Serie) sowie die Beherrschung des abstrakten Unendlichen (Teil 2) waren nur der theoretischere Teil seines Werks. Auf der praktischen Seite stehen nicht nur seine Arbeiten zur Experimentalphysik (Teil 3), sondern, noch handfester, auch die Beschäftigung mit merkwürdigen

Zahnradern und anderen mechanischen Bauteilen. Leibniz hat – neben vielen anderen Dingen – zwei geradezu visionäre Maschinen entworfen, die »Machina arithmeticata« zum Rechnen und die »Machina decipratoria« zum Ver- und Entschlüsseln von Texten.

Zu seinen Lebzeiten hat die Rechenmaschine trotz intensiver Bemühungen nie richtig funktioniert, und die Chiffriermaschine ist nie gebaut worden. Das lag bei der Rechenmaschine nicht etwa daran, dass Leibniz beim Entwurf etwas falsch gemacht hätte. Für die Chiffriermaschine fand sich kein zahlender Interessent, vermutlich weil die Diplomaten der damaligen Zeit die Sicherheit ihrer etablierten Geheimverfahren überschätzten und daher keinen Aufwand für eine Verbesserung treiben mochten. Die Rechenmaschine ist daran gescheitert, dass die Mechaniker die geforderte Präzision bei der Fertigung der Bauteile nicht erreichten. Aber so wie Leibniz seine Maschinen entworfen hat, waren sie funktionsfähig. Wir wissen das, weil wir sie unter meiner Leitung nachgebaut haben. In der mehrjährigen Auseinandersetzung mit dieser Maschine und mit einer Rekonstruktion der Chiffriermaschine habe ich eine Reihe überraschender Erkenntnisse gewonnen.

Leibniz war nicht der Erste, der sich an einer Rechenmaschine versuchte. Schon 1623 hatte der Tübinger Mathematiker und Mechaniker Wilhelm Schickard (1592–1635) eine

## SERIE

### Gottfried Wilhelm Leibniz (1646–1716)

- Teil 1: Juli 2016  
**Die vernünftig geordnete Welt** von Hans Poser
- Teil 2: Juli 2016  
**Vertreibung der Gespenster** von Thomas Sonar
- Teil 3: August 2016  
**Die perfekte Wasseruhr und das Prinzip der kleinsten Wirkung** von Hartmut Hecht
- Teil 4: September 2016  
**Die Vorfahren der Enigma und des Computers** von Klaus Badur





GOTTFRIED WILHELM LEIBNIZ BIBLIOTHEK, NIEDERSÄCHSISCHE LANDESBIBLIOTHEK, HANNOVER  
DIE VIER SPITZEN RECHENMASCHINE

### Die Machina arithmeticorum

Dies ist wahrscheinlich das einzige Exemplar von Leibnizens Arbeiten im Bereich der Mechanik, das gegenständlich erhalten geblieben ist. Heute steht die Maschine in der Gottfried Wilhelm Leibniz Bibliothek in Hannover.

Maschine gebaut, die mechanisch addieren konnte und zum Multiplizieren zumindest Hilfen bereitstellte (Bild S. 78 unten). Das Gerät ging später verloren, konnte jedoch 1957 nach alten Aufzeichnungen Schickards in zwei Briefen an seinen Zeitgenossen Johannes Kepler rekonstruiert werden.

Der Mathematiker und Philosoph Blaise Pascal (1623–1662) entwickelte mit 21 Jahren die »Pascaline«, die seinem Vater, der im Steuerwesen tätig war, das Addieren der Geldbeträge erleichtern sollte (Bild S. 78 oben). Mit ihr konnte man bis zu achtstellige Zahlen addieren und – über ein Hilfsverfahren namens Komplementbildung – auch subtrahieren. Die Maschine wurde in mehreren Exemplaren gebaut.

Noch in Mainz hatte Leibniz von der Pascaline gehört und 1671, also im Alter von 25 Jahren, erste Ideen zu einer Rechenmaschine formuliert. »Denn es ist ausgezeichneter Männer unwürdig, ihre Zeit mit sklavischer Rechenarbeit zu

verlieren, die mit Anwendung der Maschine jedem beliebigen mit Sicherheit übertragen werden könnte«, schrieb er. Die Pascaline, die er etwas abwertend als »Rechenkästchen« bezeichnete, wollte er ergänzen und übertreffen: Neben der Addition und der Subtraktion sollte seine Maschine auch multiplizieren und dividieren können. Der vorgeblichen Geringschätzung zum Trotz hat er 1672 in Paris die Pascaline eingehend studiert und in seinen Aufzeichnungen detailliert beschrieben.

### Die Machina arithmeticata

Seine eigene Maschine sollte einfach zu bedienen sein (ein »Kinderspiel«), unabhängig von der Geschicklichkeit des Bedieners zuverlässig rechnen und insbesondere für eine Multiplikation nur eine Kurbelumdrehung benötigen. Dies hätte jedoch aufwändige Übersetzungsgtriebe erfordert und wäre mit der pascalschen Konstruktion nicht vereinbar gewesen. Wohl deswegen hat Leibniz dieses Ziel nicht weiterverfolgt.

Stattdessen arbeitete er eigene Ideen aus und fand in dem hervorragenden Uhrmacher Olivier einen überaus kompetenten Partner. In der damaligen Zeit war ein Mechaniker gleichzeitig auch Konstrukteur. In diesem Fall hatte Olivier keine leichte Aufgabe, denn Leibniz war ein Kopfmensch, und da er sehr klare Vorstellungen hatte, hielt er es für eine Kleinigkeit, seine kargen und ungenauen Skizzen (Bild S. 80) in ein funktionierendes Gerät umzusetzen.

Ein erstes Modell, wahrscheinlich aus Holz, von dem keine genaue Beschreibung vorliegt, stellte Leibniz 1673 der Royal Society in London vor. Auch wenn er viele Funktionen daran noch nicht vorzeigen konnte, waren die Herren der Gelehrtengesellschaft von seiner Präsentation so beeindruckt, dass sie ihn gegen das Versprechen, demnächst eine vollständige Maschine vorzuführen, als Mitglied in die Gesellschaft aufnahmen.

Im Jahr 1675 präsentierte er der Académie des sciences in Paris ein zweites Modell, das Olivier wohl schon aus Messing gefertigt hatte. Auch diese Gesellschaft nahm ihn



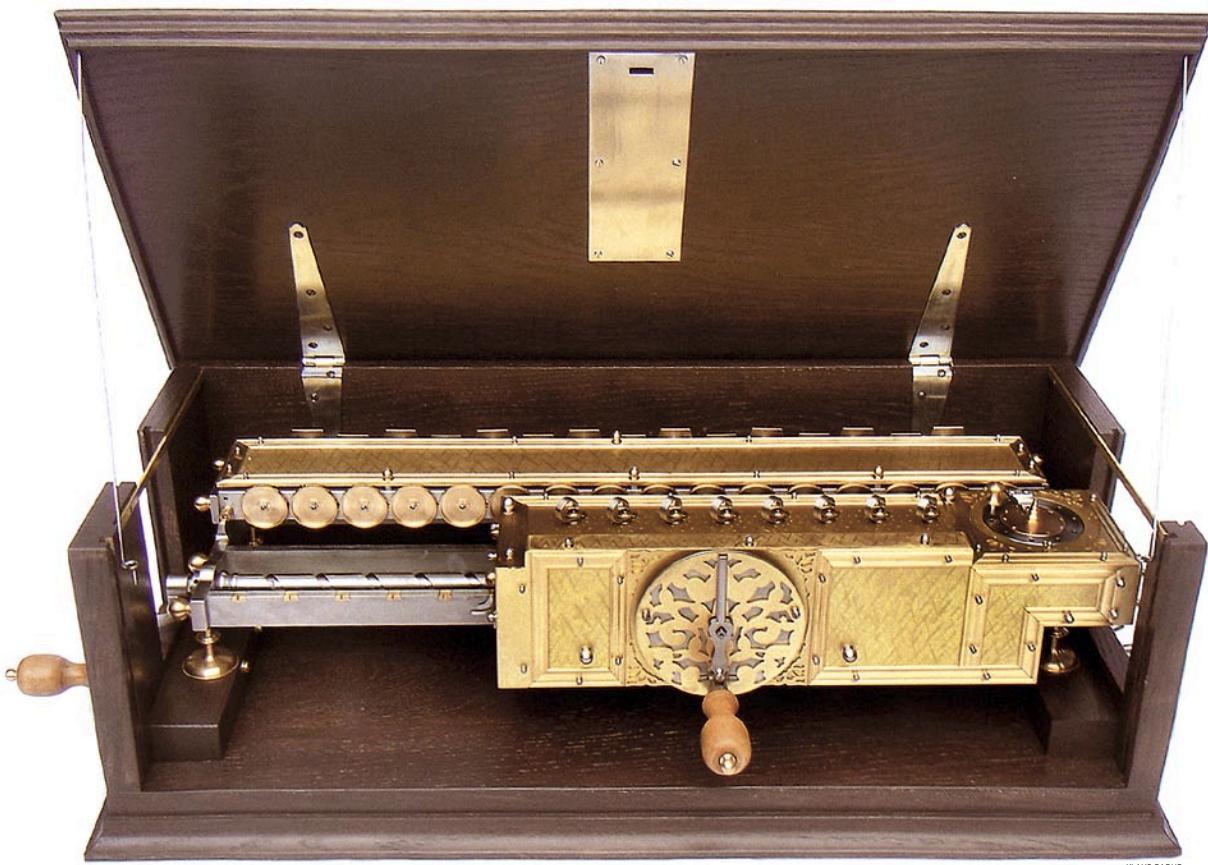
### Die Pascaline

Einige Originale der Rechenmaschine von Blaise Pascal sind erhalten geblieben und im Pariser Musée des Arts et Métiers ausgestellt. Hier abgebildet ist ein Nachbau.



### Wilhelm Schickards Rechenmaschine

Diese Maschine konnte in ihrem unteren Teil addieren und subtrahieren. Zur Multiplikation mehrstelliger Zahlen konnte man durch die Schieber im oberen Teil die Zwischenprodukte einstellen; die Methode ist von den »neperschen Rechenstäben«, Hilfsmitteln für die schriftliche Multiplikation, hergeleitet. Die so erhaltenen Zwischenergebnisse konnte man ablesen und im unteren Teil der Maschine aufzaddieren. Das Ergebnis stand auf separaten Zahlenscheiben zur Verfügung. Die hier gezeigte Rekonstruktion ist im Arithmeum in Bonn ausgestellt.



KLAUS BADUR

**Nachbau der Machina arithmeticica** durch Spektrum-Autor Klaus Badur und Wolfgang Rottstedt.

in ihre Reihen auf, allerdings erst 1700 und auf Grund seiner Arbeiten aus dem physikalischen Bereich.

Nachdem Leibniz 1676 seinen Dienst als Hofrat und Bibliothekar des Herzogs Johann Friedrich in Hannover angetreten hatte, setzte er dort ab 1680 die Arbeiten an der Rechenmaschine fort. In der Zeit wurde eine von Olivier begonnene erste vollständige Maschine mit acht Eingabestellen und zwölf Ergebnisstellen fertig gestellt. Sie wird in der Literatur als die ältere, kleine Maschine bezeichnet und ist verschollen.

Die 1690 begonnene Nachfolgerin (siehe das Bild auf S. 76/77) sollte mit acht Eingabe- und 16 Ergebnisstellen größer werden. Ihre Geschichte ist lang und enttäuschend, vor allem für Leibniz selbst, der insgesamt etwa 24 000 Taler (was heute ungefähr ein bis zwei Millionen Euro entspräche) in sein Werk investiert hatte und bis zu seinem Lebensende keinen durchschlagenden Erfolg verzeichnen konnte. Verschiedene Mechaniker fertigten Einzelteile, jetzt allerdings ohne Oliviers Beteiligung. Ab 1700 übernahm der Helmstedter Mathematikprofessor Rudolf Christian Wagner (1671–1741) die Leitung der weiteren Arbeiten. Die Mechaniker hatten größte Schwierigkeiten, die Einzelteile mit der geforderten Präzision herzustellen. Außerdem mussten viele Elemente immer wieder geändert und neu gefertigt werden. In einem Schreiben an Leibniz berichtet Wagner 1706 jedoch ausführlich von erfolgreich durchgeföhrten Rechnungen. Dennoch wollten vor allem die Zehnerüberträge im Rechenwerk nicht richtig funktionieren. Leibniz drängte

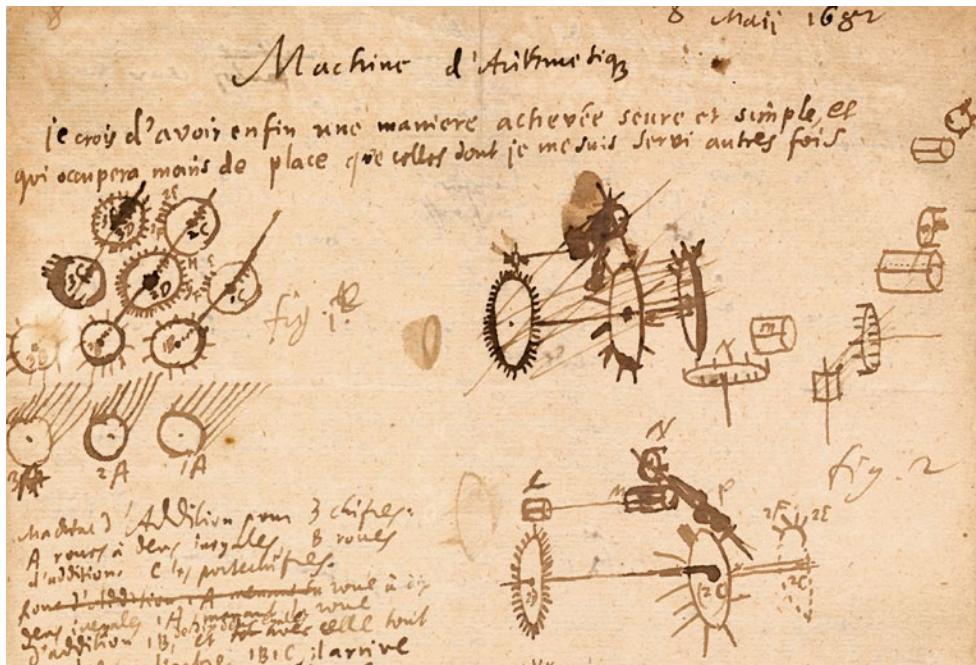
ungeduldig auf die Fertigstellung, weil er endlich seine Erfindung funktionsfähig den Herrscherhäusern Europas präsentieren wollte.

Auch als ab 1710 die Arbeiten in Zeitz unter der Leitung des dortigen Mathematikers Gottfried Teuber fortgesetzt wurden, gelang es nicht, die Maschine zufriedenstellend zum Funktionieren zu bringen. Bis zu Leibnizens Tod 1716 arbeiteten verschiedene Werker immer wieder an Verbesserungen.

## AUF EINEN BLICK LEIBNIZENS MASCHINEN

- 1** Leibniz hat eine Rechenmaschine konzipiert und über Jahrzehnte versucht, sie zum Funktionieren zu bringen. Aber die Feinmechanik seiner Zeit konnte den Entwurf schlüssig noch nicht umsetzen.
- 2** Eine Maschine zum Ver- und Entschlüsseln geheimer Nachrichten ist über das Entwurfsstadium nicht hinausgekommen, weil die potenziellen Abnehmer keinen Bedarf sahen.
- 3** Der Nachbau beider Geräte hat den Beweis erbracht, dass Leibnizens Ideen nicht nur in die Realität umsetzbar, sondern ihrer Zeit sehr weit voraus waren.

**Skizze einer Rechenmaschine**  
 »Endlich glaube ich ein sicheres und einfaches Verfahren erreicht zu haben, das auch noch weniger Platz beansprucht als diejenigen, die ich bis jetzt verfolgt habe«, so Leibniz in dieser Notiz vom 8. Mai 1682. Einem Uhrmacher blieb es überlassen, die zugehörigen Zeichnungen in eine funktionierende Mechanik umzusetzen.



GOTTFRIED WILHELM LEIBNIZ BIBLIOTHEK, NIEDERSÄSSISCHE LANDESBIBLIOTHEK HANNOVER [H.XII.4.1 Bl. 40r]

rungen im Bereich der Zehnerüberträge. Später wurde die Maschine eingelagert und tauchte erst 1880 in Göttingen wieder auf (siehe »Das Schicksal der leibnizschen Rechenmaschine«, rechts).

Dieses Scheitern könnte das ganze Unternehmen als grundsätzlich verfehlt erscheinen lassen – was ein völlig falscher Eindruck wäre. Wesentliche Elemente der leibnizschen Maschine sind in den mechanischen Rechenmaschinen, die ab etwa 1850 bis in die 1960er Jahre hinein massenhaft in Gebrauch waren, verwirklicht worden: insbesondere die Staffelwalze, die Trennung von Eingabe- und Rechenwerk, die Verschiebbarkeit des Eingabewerks zurstellenrichtigen Ausführung der Multiplikation und die Aufteilung des Zehnerübertrags in zwei Stufen.

Damals jedoch waren die Anforderungen kaum zu bewältigen, die insbesondere die Zehnerübertragsmechanik an die Fertigungsgenauigkeit stellte. An insgesamt 1650 Zahnräderpaarungen müssen die Maße auf hundertstel Millimeter genau eingehalten werden, und die Orientierung der einzelnen Wellen darf höchstens um 0,1 Grad von der exakten Position abweichen. Nur so ist eine störungsfreie Funktion zu gewährleisten. Es überrascht kaum, dass die Hersteller mit diesen Anforderungen Probleme hatten.

#### Die Leibniz-Rechenmaschine arbeitet auch ohne konstruktive Änderungen stets korrekt

Insgesamt sind 14 Nachbauten der Rechenmaschine bekannt. Einige Konstrukteure, darunter Nikolaus Joachim Lehmann (1921–1998), der Computerpionier der DDR, und Erwin Stein, Professor für Technische Mechanik in Hannover, haben die Konstruktion der Maschine selbst – erfolgreich – geändert, um den problematischen Zehnerübertrag zu verbessern. Allerdings wird die Maschine dadurch wesentlich komplizierter, und die Einzelteile müssen noch genauer justiert werden. Darüber hinaus hat Stein zusammen mit dem Getriebespezialisten Franz Otto Kopp (1937–2015) eine detaillierte mathematische Analyse der leibnizschen Konstruktion durchgeführt und deren Ergebnisse in den Bau einer optimierten Vorführmaschine im Maßstab 2:1 übernommen.

Dagegen haben der Mechanikermeister Wolfgang Rottstedt und ich uns bei unserem Projekt für einen originalgetreuen Nachbau entschieden, um das komplexe Gerät möglichst detailliert zu untersuchen. In mehreren Sitzungen fertigten wir mehr als 200 Fotos vom Original an, zum Teil mit einem Spiegel, um auch alle Einzelteile zu erfassen, die nicht von außen erreichbar waren. Das Original durfte dabei nicht betätigt oder gar demontiert werden.

Anhand dieser Informationen entstand dann ein vollständiger, normgerechter Zeichnungssatz. Anschließend haben wir in mehr als 1500 Stunden die über 650 Einzelteile der Maschine gefertigt und montiert (Bild S. 79).

Mit fortschreitender Arbeit wuchs unser Respekt vor der Leistung von Leibniz als Ideengeber und vor seinen Mechanikern, die als Konstrukteure und Fertiger die Ideen umgesetzt hatten. Mit welchen geringen Mitteln hatten diese Leute vor mehr als 300 Jahren eine solch großartige Maschine gefertigt! Es gab ja damals nur einfache Bohrmaschinen und Drehbänke mit manuellem Antrieb. Alles andere musste man mit der Feile erledigen. Heute sind diese Genauigkeitsanforderungen mit modernen Werkzeugmaschinen zu bewältigen.

Die Arbeit wurde belohnt. Mit dem originalgetreuen Nachbau konnten wir nachweisen, dass die Maschine bei ausreichend genauer Fertigung und geringer Erweiterung des Rechenalgorithmus ohne konstruktive Änderung am Konzept vollständig und korrekt rechnet (siehe »Die Funktion der leibnizschen Rechenmaschine«, S. 82/83).

Neben den extremen Genauigkeitsanforderungen ist das Projekt der leibnizschen Rechenmaschine damals sicherlich auch daran gescheitert, dass mehrere Mechaniker nacheinander an der Maschine gearbeitet haben und Leibniz sie nur sehr selten persönlich in Augenschein genommen hat. Aber es war wie bei anderen seiner genialen Ideen nicht ein Scheitern des Konzepts, sondern nur der Umsetzung. Leibniz war auch hier seiner Zeit weit voraus.

Als Leibniz seine Rechenmaschine der Royal Society präsentierte, stellte ein Mitglied den Sinn eines solchen Geräts in Frage. Es sei ja sehr umständlich zu bedienen, und schriftlich, von Hand, würde man schneller und einfacher

rechnen. Heute erscheint dieser Einwand vollends anachronistisch; man bedenke jedoch, dass unsere heutigen Computer im Grunde nur Weiterentwicklungen der leibnizschen Ideen sind.

### **Die Machina deciphatoria nahm moderne Methoden der Verschlüsselung um Jahrhunderte vorweg**

Die Technik der Ver- und Entschlüsselung war für Leibniz schon von Berufs wegen relevant. Immerhin hatte er als Diplomat häufig geheime Nachrichten zu versenden, zu übermitteln und zu empfangen. Er hat sich jahrelang sehr ausführlich mit dem Thema Kryptografie beschäftigt und eine Reihe bedeutender wissenschaftlicher Erkenntnisse gewonnen, wie viele seiner erhaltenen Aufzeichnungen und Briefe belegen. Das Material ist sehr umfangreich und noch nicht erschöpfend ausgewertet.

Im Verkehr mit seinen Briefpartnern verwendete Leibniz unter anderem eine Verschlüsselung, die einfach durchzuführen ist und nur erfordert, dass beide Partner ein einziges Wort (das »Schlüsselwort«) als Geheimnis teilen. Man schreibe in ein Schema mit 2 mal 13 Kästchen zunächst das Schlüsselwort, in diesem Beispiel »LABYRINTHUS«, und dann alle noch nicht verwendeten Buchstaben des Alphabets in der üblichen Reihenfolge:

L	A	B	Y	R	I	N	T	H	U	S	C	D
E	F	G	J	K	M	O	P	Q	V	W	X	Z

Zum Verschlüsseln ersetzt man jeden Buchstaben durch denjenigen, der unmittelbar darunter- oder darübersteht; zum Entschlüsseln verfährt man genauso. Zum Beispiel wird aus dem Klartext

**LEIBNIZ MACHINA ARITHMETICA**  
der Chiffretext

**ELMGOMD IFXQMOF FKMPQILPMXF.**

Eine derartige Verschlüsselung würde allerdings einem Angriff nicht lange standhalten. Denn die Zuordnung von Klartext- und Chiffretextbuchstaben ist eindeutig; zum Beispiel wird aus einem I immer ein M. Daher führt eine schlichte Häufigkeitsanalyse meistens schon zum Ziel. Der häufigste Buchstabe des Chiffretextes entspricht – nicht in diesem kurzen Beispiel, aber in der Regel – dem Klartextbuchstaben E, weil dieser Buchstabe in einem (deutschen) Text am häufigsten vorkommt. Unter dieser Schwäche leiden alle monoalphabetischen Verfahren, das sind solche, die nur eine Zuordnung von den Klartext- zu den Chiffretextbuchstaben (ein »Alphabet«) verwenden.

Dem wäre durch polyalphabetische Chiffren abzuhelpfen: Man verschlüsselt den ersten Buchstaben mit einem Alphabet, den zweiten mit einem anderen, den dritten mit wieder einem anderen und so weiter. Wenn das Sortiment der Alphabete erschöpft ist, fängt man wieder von vorne an. Und damit handelt man sich eine – geringere, aber immer noch erhebliche – Schwäche ein. Wenn man beispielsweise zehn Alphabete immer wieder rundum verwendet, ist jeder zehnte Buchstabe mit demselben Alphabet verschlüsselt. Ein gewisser Rest dieser periodischen Struktur bleibt im Chiffretext erhalten und bietet Angriffsmöglichkeiten.

Für das Problem gibt es im Wesentlichen zwei Lösungen. Man arbeitet entweder mit sehr ▶ Lesen Sie weiter auf S. 84

## **Das Schicksal der leibnizschen Rechenmaschine**

- 1671–1672** Leibniz stellt erste Überlegungen zur Rechenmaschine an.
- 1672** Er übersiedelt nach Paris. Ein erstes Holzmodell entsteht.
- 1673** Präsentation des Modells bei der Royal Society in London
- 1675** Präsentation eines neuen, von Olivier aus Messing gefertigten Modells bei der Pariser Académie des sciences
- 1676** Leibniz zieht nach Hannover.
- 1979–1694** Bau einer älteren, kleinen Rechenmaschine mit acht Eingabe- und zwölf Ergebnissstellen, wahrscheinlich aus dem von Olivier gefertigten Modell
- Ab 1693** Weiterbau und Verbesserung dieser Maschine durch den Uhrmacher Georg Heinrich Köllbing
- Ab 1690** Fertigung der Einzelteile für die jüngere, große Rechenmaschine mit acht Eingabe- und 16 Ergebnissstellen
- Ab 1700** Rudolf Christian Wagner betreut die weiteren Arbeiten in Helmstedt mit dem Werker Levin und dem Schlosser Georg Warnecke.
- Ab 1701** Montage der jüngeren großen Maschine
- 1702–1710** Erprobung, Umbauten und Verbesserungen durch Levin und Warnecke an der Maschine unter der Aufsicht von Wagner
- 1710–1716** Weitere Arbeiten an beiden Rechenmaschinen in Zeitz unter Gottfried Teuber
- 1716** Nach Leibnizens Tod wird die große Maschine in Hannover eingelagert.
- 1764** Die große Maschine wird Abraham G. Kästner an der Universität Göttingen zur Untersuchung übergeben und später in der Modellkammer der Georgia Augusta eingelagert.
- Seit 1880** Die Maschine befindet sich in der heutigen Gottfried Wilhelm Leibniz Bibliothek in Hannover.
- 1894–1896** Der Rechenmaschinenfabrikant Gottfried Burkhardt restauriert die Maschine in Glashütte.

# Die Funktion der leibnizschen Rechenmaschine

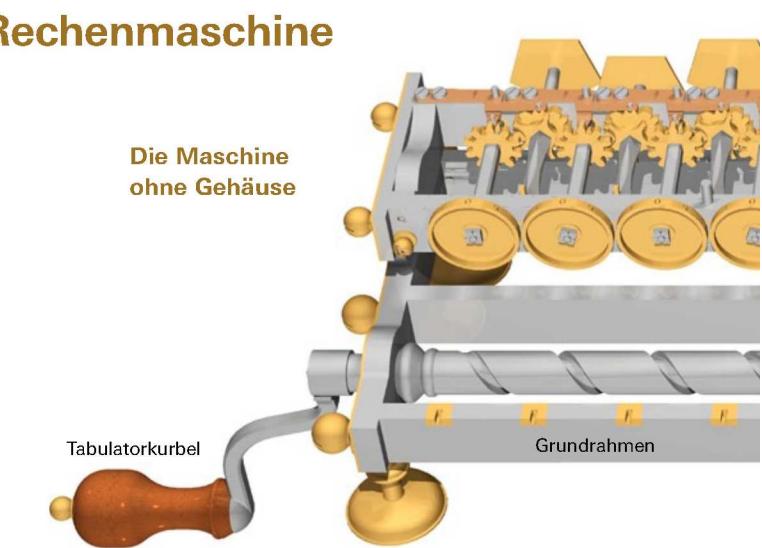
**Im Prinzip addiert die Maschine zwei Zahlen so**, wie man es in der Grundschule lernt. Man arbeitet von rechts nach links, und wenn man beim Addieren über die Neun hinauskommt, addiert man für die Zehn eine Eins in der nächsthöheren Stelle.

Am Eingabewerk der Maschine stellt man die zu addierenden Zahlen ein und überträgt sie durch eine einzige Drehung mit der Antriebskurbel (»Magna Rota«) in das Rechenwerk; dort wird sie zu dem bisherigen Inhalt des Rechenwerks hinzugefügt.

Zu Beginn der Rechnung ist das Rechenwerk auf null gesetzt. Nachdem man den ersten Summanden im Eingabewerk eingestellt und die Kurbel gedreht hat, steht dieser im Rechenwerk. Daraufhin stellt man den zweiten Summanden ein, dreht die Kurbel und findet im Rechenwerk die Summe vor, abzulesen an den Scheiben der Ergebnisanzeige.

Zum Aufaddieren dient ein spezielles Bauteil: die Staffelwalze. Leibniz hat sie erfunden und wegen ihrer speziellen Form als »Wendeltreppchen« bezeichnet. Man kann sie sich folgendermaßen aufgebaut vorstellen: Auf einer gemeinsamen Achse, der »Eingabewelle«, sitzen neun Zahnräder mit je 22 Zähnen. Aber von Zahnrad 1 sind alle Zähne bis auf einen entfernt, Zahnrad 2 hat nur zwei Zähne, und so weiter. Auch die neun Zähne von Zahnrad 9 verteilen sich nicht gleichmäßig über den Umfang, sondern lassen eine Lücke; die ist notwendig, damit der Zehnerübertrag (siehe unten) reibungslos funktioniert. Für die Ziffer Null wird die Staffelwalze außer Eingriff mit dem Rechenwerk geschoben.

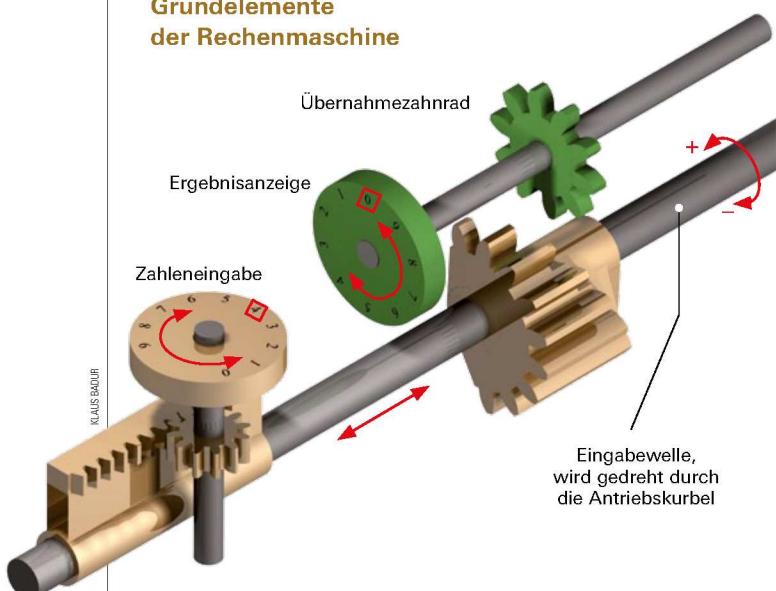
Zum Einstellen eines Summanden hebt man ein Einstellräddchen leicht an, dreht es, bis die Zeigerspitze auf die richtige Ziffer zeigt, und lässt es einrasten. Dadurch schiebt eine Zahnstange die Staffelwalze mit dem richtigen Zah-



rad unter das Übernahmезahnrad des Rechenwerks. Eine Drehung der Kurbel gegen den Uhrzeigersinn dreht das Übernahmезahnrad um die entsprechende Anzahl Zähne weiter (Bild links unten) und vollzieht dadurch die Addition. Eine Drehung in entgegengesetzter Richtung entspricht einer Subtraktion.

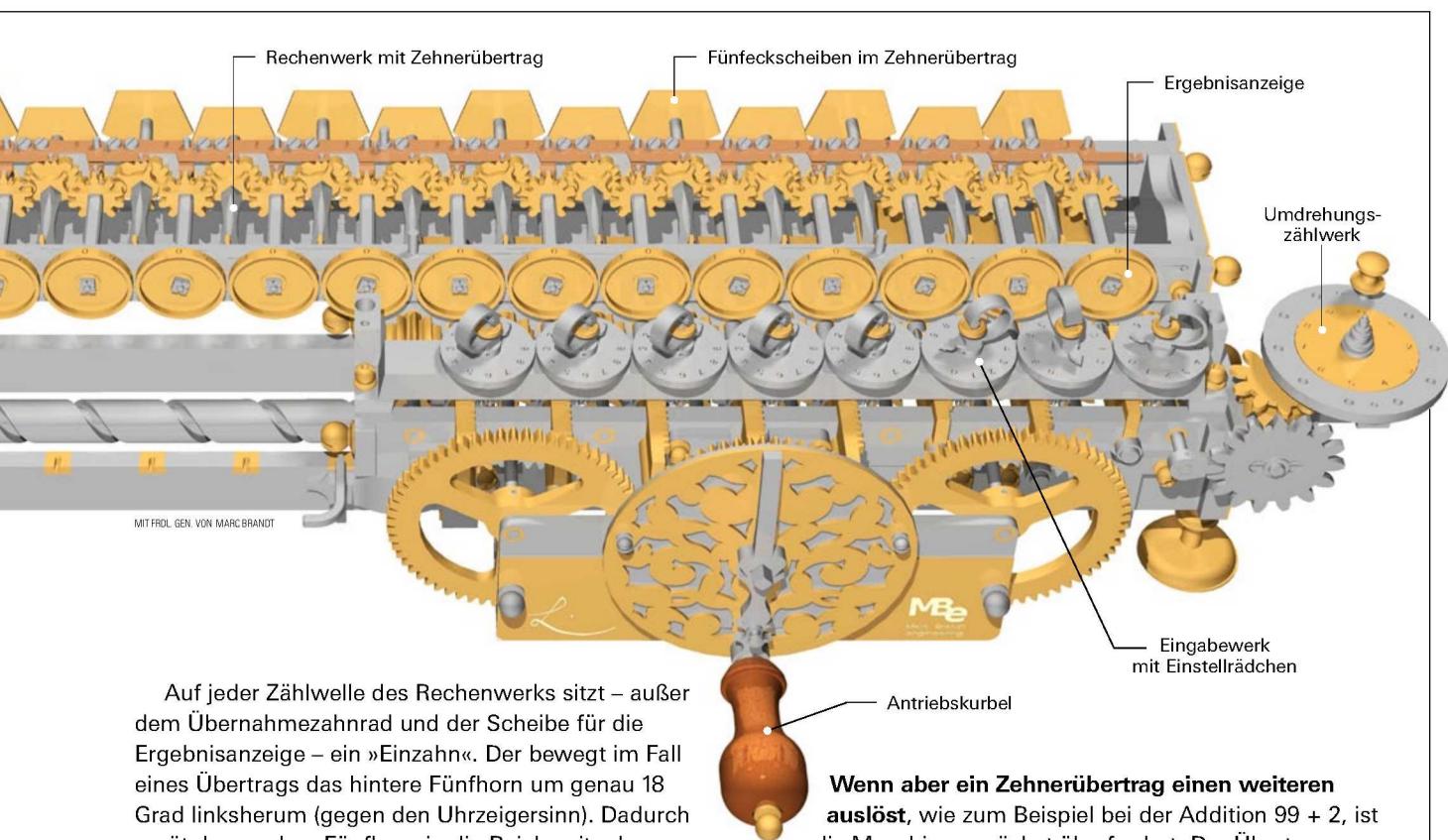
Die Multiplikation wird als wiederholte Addition ausgeführt. Man stellt den Multiplikanden im Eingabewerk ein und dreht die Kurbel so oft, wie die Einerstelle des Multiplikators angibt. Das Umdrehungszählwerk dient zur Kontrolle. Dann verschiebt man mit Hilfe der Tabulatorkurbel das gesamte Eingabewerk um eine Stelle nach links, dreht die Kurbel so oft, wie die Zehnerstelle des Multiplikators angibt, und so weiter. Auf diese Weise erfordert zum Beispiel eine Multiplikation mit 134 nicht etwa 134 Kurbeldrehungen, sondern nur  $1 + 3 + 4 = 8$ .

## Grundelemente der Rechenmaschine



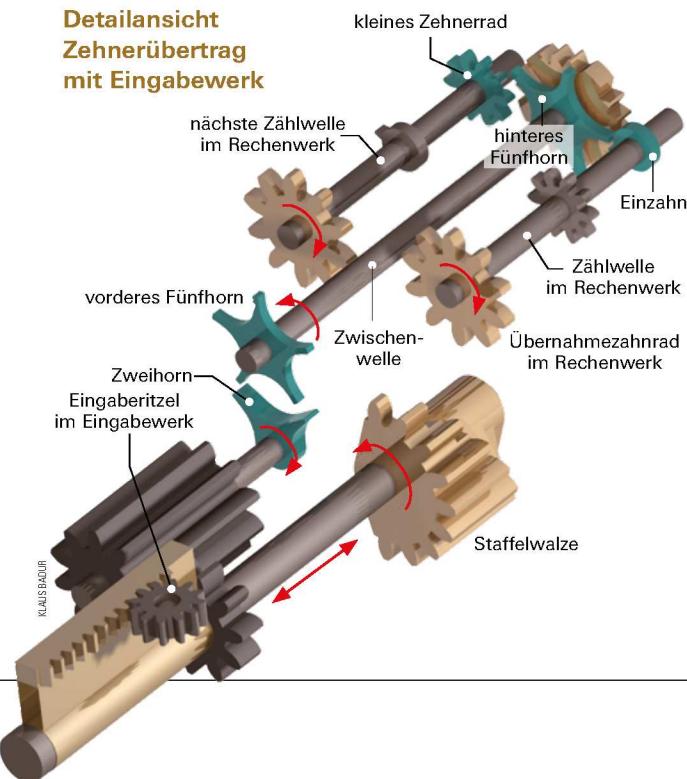
**Besondere Aufmerksamkeit erfordert der Zehnerübertrag.** Wenn beispielsweise die Addition  $39 + 42$  auszuführen ist, dann steht bereits 39 im Rechenwerk, während 42 im Eingabewerk eingestellt ist. Durch die Kurbeldrehung wird das Einerrad des Rechenwerks um zwei Zähne und das Zehnerrad um vier Zähne weitergedreht, es steht also 71 im Rechenwerk, während 81 richtig wäre.

Das Zehnerrad muss also noch um den Übertrag 1 weiterbefördert werden. Das ist aber nicht möglich, während die Staffelwalzen noch in die Übernahmезahnräder eingreifen, weil sonst alle Zahnräder blockieren würden. Also darf der Übertrag nicht gleichzeitig ausgeführt werden; vielmehr wird er in einer Warteposition zwischen gelagert und erst in der zweiten Hälfte der Kurbeldrehung vollendet, wenn die Staffelwalzen »zahnlos« sind. Dazu ist zwischen je zwei Achsen des Rechenwerks eine »Zwischenwelle« angeordnet, auf der zwei Fünfhörner angebracht sind (Bild rechts).



Auf jeder Zählwelle des Rechenwerks sitzt – außer dem Übernahmzahnrad und der Scheibe für die Ergebnisanzeige – ein »Einzahl«. Der bewegt im Fall eines Übertrags das hintere Fünfhorn um genau 18 Grad linksherum (gegen den Uhrzeigersinn). Dadurch gerät das vordere Fünfhorn in die Reichweite des Zweihorns. Dieses wiederum sitzt auf einer Welle, die von der Kurbel mitgedreht wird, und dreht nun das vordere Fünfhorn um weitere 54 Grad linksherum. Dabei dreht das hintere Fünfhorn das kleine Zehnerrad der links benachbarten Zählwelle (die für die nächsthöhere Stelle zuständig ist) um einen Zahn weiter, womit der Zehnerübertrag abgeschlossen ist. Das geschieht an allen Stellen des Rechenwerks gleichzeitig.

#### Detailansicht Zehnerübertrag mit Eingabewerk



**Wenn aber ein Zehnerübertrag einen weiteren auslöst**, wie zum Beispiel bei der Addition 99 + 2, ist die Maschine zunächst überfordert. Der Übertragsmechanismus stellt das Zehnerrädchen korrekt auf null, und dessen Einzahl bewegt die Fünfhörner der Welle zwischen Zehner- und Hunderterstelle. Aber das Zweihorn greift nicht mehr ein, denn es ist ja längst am vorderen Fünfhorn vorbeigelaufen. Also bleibt der Übertrag von der Zehner- zur Hunderterstelle unvollendet und das Ergebnis falsch.

Am hinteren Ende jeder Zwischenwelle ist eine Scheibe in Gestalt eines regelmäßigen Fünfecks angebracht. Dieses zeigt bei einem unvollendeten Übertrag mit einer Spitze nach oben. Man könnte die Situation bereinigen, indem man die entsprechenden Fünfeckscheiben von Hand ein Stück weiterdreht. So hatte es Wagner auch Leibniz vorgeschlagen – was dieser aber als »unrecht« verwarf.

Daraus wurde in der Vergangenheit der Schluss gezogen, dass die Maschine nicht korrekt arbeite. Das ist falsch, denn es gibt eine einfache Abhilfe. Wenn am Ende einer Rechnung noch unvollendete Zehnerüberträge ausstehen, stellt man die Eingabe am Eingabewerk in allen acht Stellen auf null und dreht dann die Kurbel noch ein paar Mal. Bei jeder Umdrehung werden bis zu zwei Überträge vollendet, und am Ende hat man ohne Eingriff in die Maschine das richtige Ergebnis. Schließt man an eine Rechnung eine weitere an, so erledigen die Kurbeldrehungen alle ausstehenden Überträge aus der alten Rechnung mit. Die beschriebene Bereinigung ist also nur bei der jeweils letzten aus einer Folge von Rechnungen durchzuführen.

## Die Enigma

Die Chiffriermaschine der Deutschen im Zweiten Weltkrieg arbeitet mit einem sehr komplexen und dadurch sehr schwer zu entschlüsselnden Substitutionsverfahren. Bei ihr wird die zu verschlüsselnde Nachricht über die Tastatur wie bei einer Schreibmaschine eingegeben. Mittels elektrischer Schaltkreise, die über mehrere Kontaktwalzen und Stecker nach jeder Tasteneingabe verändert werden, wird der kodierte Buchstabe im Lampenfeld angezeigt. Durch die rotierenden Kontaktwalzen ändert sich nach jedem eingegebenen Buchstaben das Geheimalphabet.



## Die Geheimnismaschine von Leibniz

Nicholas Rescher, Jahrgang 1928, ist Professor für Philosophie an der University of Pittsburgh (Pennsylvania). Neben vielen anderen Dingen beschäftigt er sich intensiv mit der Philosophie von Leibniz.

Seit der Antike dient die Verschlüsselung zur vertraulichen Übermittlung, und in der Renaissance kamen mechanische Hilfsmittel dafür in Gebrauch, darunter Alphabetschieber und -scheiben mit einer Mechanik vergleichbar derjenigen eines Rechenschiebers oder einer Rechenscheibe. Die Arbeit mit diesen Geräten war langsam, mühevoll und fehlerträchtig, so dass es sinnvoll erschien, sie an mechanische Automaten zu delegieren. Das geschah mit zunehmender Intensität im Verlauf des 20. Jahrhunderts, vorrangig für militärische und diplomatische Zwecke.

Weit früher, 1688, hatte jedoch Leibniz in einem Schriftsatz für eine Audienz bei Kaiser Leopold I. in Wien in allen Einzelheiten eine Chiffriermaschine beschrieben, die er schon seit einiger Zeit im Sinn hatte. Damit nahm er um reichlich 200 Jahre das Prinzip der Rotor-Schlüsselmaschine von Arvid Damm (1869–1927) vorweg, nach dem die erste Generation der mechanischen Chiffriermaschinen (ab 1918) funktionierte. Wie die berühmte Enigma hatte Leibnizens Maschine eine Tastatur zur Eingabe von Buchstaben, die zugleich das Chiffrieralphabet weiterschaltete, und eine Anzeige für das Ergebnis. Allerdings war, der Zeit entsprechend, die Tastatur nicht von der Schreibmaschine inspiriert, sondern vom Klavier, und die Anzeige nicht elektrisch, sondern mechanisch. Nicht eine Elektronik wechselte für den jeweils nächsten Buchstaben in möglichst undurchschaubarer Weise die Verschlüsselung, sondern die Staffelwalze, die Leibniz bereits für seine Rechenmaschine verwendet hatte.

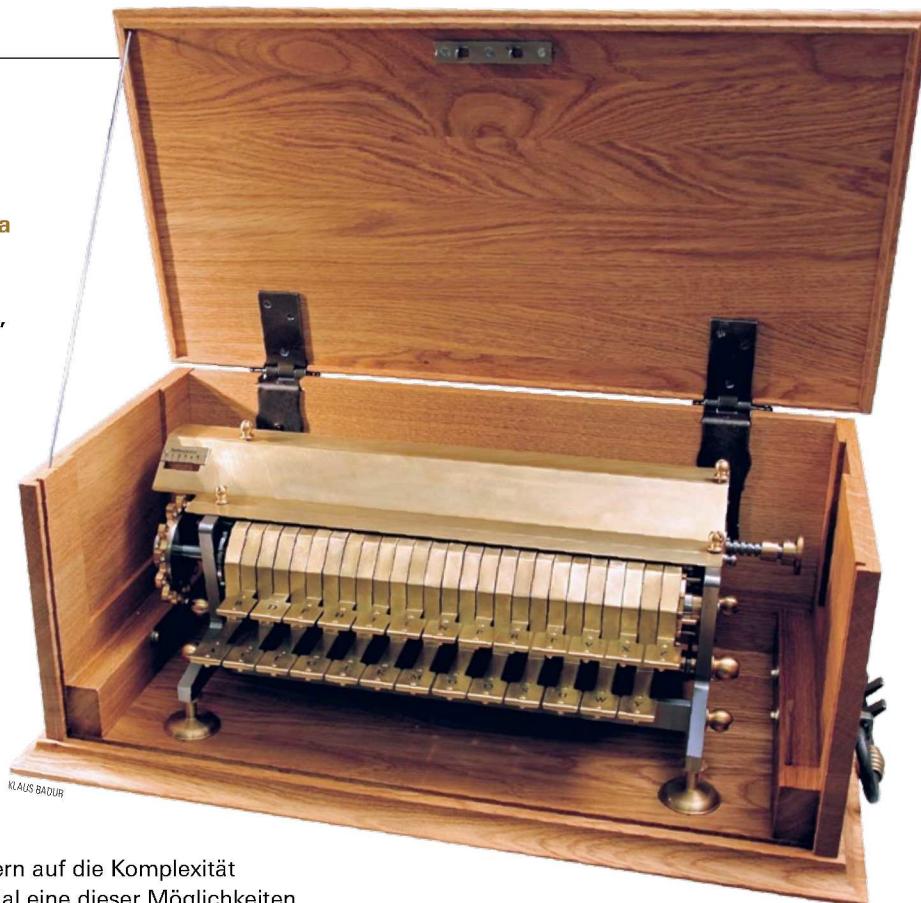
Wie alle späteren kryptografischen Maschinen stellte auch Leibnizens Gerät eine ungeheure Anzahl an Verschlüsselungsmöglichkeiten bereit. Aber diese Angabe ist geeignet, die Anwender in falscher Sicherheit zu wiegen. Es kommt nämlich nicht auf die schiere Anzahl

► Fortsetzung von S. 81 vielen Alphabeten, mehr, als die typische Nachricht Zeichen hat, so dass es keine für den Kodeknacker nutzbaren Wiederholungen gibt. Oder man beschränkt sich auf eine überschaubare Anzahl von Alphabeten, wechselt diese aber in einer völlig undurchschaubaren Folge ab.

Nach dem ersten Prinzip funktionierte die Enigma (Bild links), jene Maschine, welche die Deutschen im Zweiten Weltkrieg verwendeten und für unknackbar hielten – ein Irrtum, der erst 30 Jahre später aufgeklärt wurde. Die Enigma erzeugte das von Buchstabe zu Buchstabe neue Alphabet durch eine Art Zählwerk, dessen Stellung über

### Die Machina deciphatoria

Nicholas Rescher hat das Prinzip aus Leibnizens Aufzeichnungen rekonstruiert, Klaus Badur den Entwurf in ein funktionierendes Gerät umgesetzt.



der Möglichkeiten an, sondern auf die Komplexität des Verfahrens, das jedes Mal eine dieser Möglichkeiten auswählt, und vor allem auf das – neue und bisher nicht praktizierte – Verfahren selbst.

Genau daran ist die Enigma im Zweiten Weltkrieg gescheitert. Die ursprüngliche kommerzielle Version aus den 1920er Jahren wurde schrittweise verbessert, indem man neue Elemente einführte – aber immer nur eines auf einmal. Mit allen Neuerungen zugleich ausgestattet, wäre sie vielleicht unüberwindlich gewesen; aber so konnten zuerst die Polen, später die Briten mit jeder der kleinen Verbesserungen mithalten. (Die größte unter ihnen war die Einführung eines vierten Rotors in die Marineversion der Enigma.) Dagegen hat die astronomisch hohe Zahl an Verschlüsselungsmöglichkeiten nicht geholfen.

Kaiser Leopold hat Leibnizens Angebot damals nicht angenommen, weil seine Berater ihre etablierten Verfahren (fälschlich) für sicher hielten. Gleichwohl war Leibnizens

elektrische Kontakte ausgewertet wurde (**Spektrum** Juni 1999, S. 26). Ein entsprechendes Verfahren wäre zu Leibnizens Zeiten kaum praktikabel gewesen. An Stelle des Zählwerksmechanismus hätten beide Seiten mit umfangreichen Papierlisten arbeiten müssen.

Leibniz wählte daher den zweiten Weg. Aber auch wenn sich dabei der Umfang des zum Chiffrieren benötigten Materials in Grenzen hielt, blieben sowohl das Verschlüsseln als auch das Entschlüsseln mühsame und fehlerträchtige Tätigkeiten. So lag es nahe, diese Arbeit an eine Maschine zu delegieren. Zur Vorbereitung einer Audienz bei Kaiser Leopold I. in Wien schrieb Leibniz 1688:

Maschine eine geniale Errungenschaft, die selbst die Enigma in den Schatten stellte. Mit der irregulären Alphabetumschaltung durch die Staffelwalze hätte Leibniz die Kryptografie weiter vorangebracht, als sich irgendjemand anders hätte denken können – damals und noch mehr als 200 Jahre danach. Höchstwahrscheinlich hätte die moderne Theorie – ohne Computer und bei den damals geringen Datenmengen – den besten Kodeknackern nicht gegen diese Maschine geholfen.

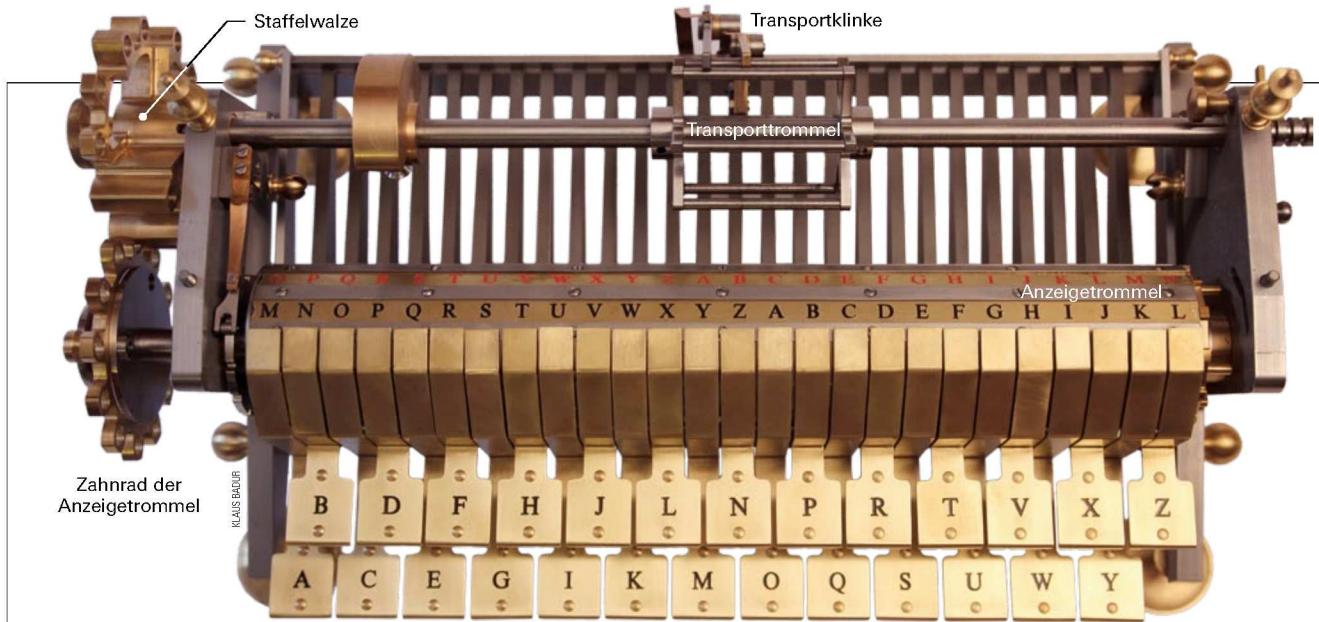
#### QUELLEN

**Rescher, N.:** Leibniz and Cryptography. Kapitel 17 in: On Leibniz. Expanded Edition. University of Pittsburgh Press, 2013

**Winkel, B. J. et al. (Hg.):** The German Enigma Cipher Machine. Artech House, Boston /London 2005

»Dergleichen sind meine Machina deciphatoria damit ein potentat mit vielen ministris, in unterschiedlichen ziphern gleich correspondiren, und ohne einige muhe entweder die zipher die er schreiben will, und den verstand dessen so ihm in zipher zugeschickt wird gleichsam wie auff einem musicalischen instrument oder clavicordio greffen könne, also dass es gleich mit berührung der clavir darstehe, und nur abcopiret werden dürffe.«

Auch in der Korrespondenz mit Herzog Johann Friedrich beschreibt er seine Ideen zu einer Chiffriermaschine. Ob er selbst den Bau einer solchen Maschine weiter betrieben hat,



## Die Machina deciphratoria – Umschaltmechanismus

Im vorderen Bereich befinden sich 26 Tasten zur Eingabe der Buchstaben von A bis Z. Wer Zahlen übermitteln will, muss sie wie bei der Enigma in Buchstaben ausschreiben.

Ein Tastendruck (im gezeigten Beispiel G) gibt erstens den Blick auf einen Buchstaben (hier ein rotes Y) frei.



Dieser gehört zu einem Streifen, der seinerseits auf einer quer liegenden Anzeigetrommel befestigt ist. Die Anzeigetrommel hat auf ihrem Umfang Platz für sechs Paare von Streifen. Ein Streifen eines Paars enthält in schwarzer Schrift die Geheimbuchstaben, die an die Stelle der Klartextbuchstaben A, B, C, ... treten sollen, der andere führt in roter Schrift der Reihe nach zu jedem Geheimbuchstaben den richtigen Klartextbuchstaben auf. Auf der Trommel sind immer ein schwarzer und der zugehörige rote Streifen untereinander angeordnet. Welcher von beiden angezeigt wird, hängt davon ab, ob das Zahnrad der Anzeigetrommel auf C (Chiffrieren) oder D (Dechiffrieren) eingestellt ist (Bild rechts oben).

Zweitens dreht auf einen Tastendruck hin eine Transportmechanik aus Transporttrommel und Transportklinke die Staffelwalze um 60 Grad. Wie in der Rechenmaschine kann man sich dieses Bauteil als mehrere – diesmal fünf – aufeinandergelegte Zahnräder auf einer gemeinsamen Achse vorstellen. Diesmal allerdings liegen die zwölf Zähne im Prinzip gleichmäßig über den gesamten Umfang verteilt. Auch hier fehlen Zähne, aber nicht so systematisch wie bei der Rechenmaschine, sondern ungeordnet.

ist nicht bekannt. Aber es ist anzunehmen, dass er mit den Kenntnissen, die er bei den Arbeiten an seiner Rechenmaschine gewonnen hatte, sehr wohl ein solches Projekt erfolgreich hätte durchführen können.

Immerhin waren seine Aufzeichnungen so aussagekräftig, dass es gelungen ist, sie in eine praktikable Bauanleitung umzusetzen. Nicholas Rescher, Professor für Philosophie an der University of Pittsburgh (Pennsylvania), beschäftigt sich seit vielen Jahren mit Leibniz und seiner Kryptografie (siehe seinen Beitrag »Die Geheimnismaschine von Leibniz«, S. 84/85). Zusammen mit dem Ingenieur Richard Kotler hat er einen detaillierten Konstruktionsentwurf erstellt. Nach

diesen Vorgaben wurden unter meiner Leitung Detailkonstruktionen erstellt und zwei dieser Maschinen in Hannover gefertigt (Bild S. 85 oben). Eine der Rekonstruktionen befindet sich heute in Pittsburgh, die zweite in einer Dauerausstellung der Leibniz Universität Hannover.

Vorbild für die Ausführung war dabei das vorhandene Original der Leibniz-Rechenmaschine. Insbesondere haben wir uns bei einem zentralen Bauteil, der Staffelwalze, von ihrer Verwendung in der Rechenmaschine leiten lassen. Durch die Lücken in ihrer Zahnrreihe erzeugt die Staffelwalze einen unregelmäßigen Wechsel unter den verschiedenen Chiffrieralphabeten. Da sie gewissermaßen aus fünf ver-



### Die Staffelwalze

**Links ein Computermodell,**  
**oben links die Staffelwalze**  
**eingreifend in das Zahnrad**  
**(oben rechts).**

Durch seitliche Verschiebung der Staffelwalze kann man einstellen, welches ihrer fünf lückenhaften Zahnräder wirksam ist, das heißt in das Zahnrad der Anzeigetrommel eingreift.

Je nachdem, ob die Staffelwalze in ihrer gegenwärtigen Position Zähne oder Lücken hat, treibt sie ein Zahnräder, das mit der Anzeigetrommel verbunden ist, ebenfalls um 60 Grad (zwei Zähne) weiter oder auch nicht. Durch den Tastendruck wird also einerseits der nächste ver- oder entschlüsselte Buchstabe angezeigt (und der Anwender muss ihn auf Papier notieren), andererseits das Verschlüsselungsalphabet durch das jeweils nächste ersetzt – oder auch nicht.

Da die Anzeigetrommel für das Chiffrieren wie für das Dechiffrieren nur sechs verschiedene Stellungen hat, bräuchten die Staffelwalze und das zugehörige Zahnräder eigentlich nur je sechs Zähne (bei der Staffelwalze die Lücken mitgezählt). Dadurch würden aber die wenigen Zähne im Vergleich zum Rest des Rads ungünstig groß und würden nicht mehr gut aneinander abgleiten. Deswegen ist gewissermaßen jeder der sechs großen Zähne durch zwei gleiche kleine ersetzt worden.

schiedenen, in unterschiedlicher Weise lückenhaften Zahnrädern besteht, kann man dem Angreifer durch Wechsel von einem Zahnräder zum anderen das Geschäft zusätzlich erschweren (siehe »Die Machina deciphatoria – Umschaltmechanismus«, oben).

Damit die geheime Nachrichtenübermittlung funktioniert, müssen Sender und Empfänger der Nachricht über identische Maschinen verfügen und vorab einen »Schlüssel« verabreden. Dieser beschreibt diejenige unter den vielen möglichen Einstellungen der Maschine, die beide Beteiligten für eine konkrete Nachrichtenübermittlung anzuwenden haben. Typischerweise legt man für jeden Tag der abseh-

baren Zukunft, zum Beispiel für das nächste Jahr, einen Schlüssel fest. Dieses Schlüsselverzeichnis nimmt der Diplomat im versiegelten Umschlag mit, wenn er in sein Gastland entsandt wird, und hütet es sorgfältig. Die chiffrierte Nachricht selbst kann dann »über einen unsicheren Kanal« verschickt werden, also über einen Weg, auf dem ein Gegner sie kopieren kann: heute das Internet, damals die gewöhnliche oder auch die Diplomatenpost.

Für die leibnizsche Maschine besteht der Schlüssel aus

- ▶ einem Sortiment von sechs Chiffrieralphabeten, die mitsamt den zugehörigen Dechiffrieralphabeten auf die Trommel aufzubringen sind;
- ▶ der Angabe, welches von zwölf möglichen Lückenzahnrädern zum Einsatz kommt;
- ▶ der Anfangsposition dieses Lückenzahnrads.

Für die sechs Chiffrieralphabete hat man im Prinzip die Auswahl aus  $26! = 1 \cdot 2 \cdot \dots \cdot 26 \approx 4 \cdot 10^{26}$  Möglichkeiten.

Realistischerweise hätte man dem Diplomaten wohl kaum mehr als 50 Alphabetpaare in den Geheimkoffer gegeben. Aber solange der Spion nicht an den Koffer kommt, muss er das komplette Sortiment der Möglichkeiten in Betracht ziehen. Und selbst mit 50 Alphabetpaaren bleiben  $50! / (50 - 6)! = 11\,441\,304\,000$  Möglichkeiten, sie auf der Trommel zu montieren – die Reihenfolge der Streifen mitgerechnet.

Das jeweils zuständige Zahnräder aus dem Sortiment, das die Staffelwalze bietet, stellt man ein, indem man die Staffelwalze entlang der Trommelachse verschiebt und möglicherweise die ganze Staffelwalze auswechselt.

Insgesamt hätte Leibnizens Chiffriermaschine sowohl nach der Zahl der möglichen Geheimalphabete als auch nach der Schwierigkeit der Entschlüsselung durchaus mit der modernen Enigma mithalten können. ◀

### QUELLEN

**Badur, K., Rottstedt, W.:** Und sie rechnet doch richtig! Erfahrungen beim Nachbau einer Leibniz-Rechenmaschine. In: *Studia Leibnitiana* 36, S. 129–146, 2004

**Breger, H.:** Zwischen Philosophie, Mathematik und Politik: Leibniz und die Kryptographie. In: Herbst, J. et al. (Hg.): Einheit in der Vielfalt. VIII. Internationaler Leibniz-Kongress. Gottfried Wilhelm Leibniz Gesellschaft, Hannover 2006

**Von Mackensen, L.:** Die Vorgeschichte und die Entstehung der 4-Spezies-Rechenmaschine von Gottfried Wilhelm Leibniz. Dissertation, München 1968. In: *Studia Leibnitiana, Supplementa* 2, S. 34–68, 1969

**Rescher, N. et al.:** Design and Construction of Leibniz's Proposal for a Machina Deciphatoria. Erscheint in: X. Internationaler Leibniz-Kongress 2016. Gottfried Wilhelm Leibniz Gesellschaft, Hannover 2016

**Stein, E., Kopp, F.O.:** Konstruktion und Theorie der Leibnizschen Rechenmaschine im Kontext der Vorläufer, Weiterentwicklungen und Nachbauten. In: *Studia Leibnitiana* 42, S. 1–128, 2010

**Walsdorf, A. et al.:** Das letzte Original. Die Leibniz-Rechenmaschine der Gottfried Wilhelm Leibniz Bibliothek. Olms, Hildesheim 2014

**Walsdorf, A.:** Von der Idee der »Lebendigen Rechenbank« zur Konstruktion der Staffelwalze — Die erste Entwicklungsphase der Leibniz-Rechenmaschine. Erscheint in: X. Internationaler Leibniz-Kongress 2016. Gottfried Wilhelm Leibniz Gesellschaft, Hannover 2016