Leibniz Universität Hannover

Eine „Machina Deciphratoria“ nach Gottfried Wilhelm Leibniz

Referat für
Kommunikation und Marketing

Tel. +49 511 762 5342
Fax +49 511 762 5391

E-Mail: kommunikation
@uni-hannover.de

17. November 2014
im/14

Neue Chiffrier-/Dechiffriermaschine ergänzt die Leibniz-Dauerausstellung der Leibniz Universität Hannover im Sockelgeschoss des Welfenschlosses

Leibniz' Interesse an der Kryptographie

Es ist charakteristisch für Leibniz, dass er mit seinem Postulat „*Theoria cum praxi*“ für die von ihm konzipierte Berlin-Brandenburgische Sozietät der Wissenschaften (gegründet am 01. Juli 1700 in Berlin mit ihm als Präsidenten) versuchte, theoretische Erkenntnisse in praktische und nützliche Erfindungen zu übertragen, so auch in die *Machina Deciphratoria*. Man kann aufgrund des Studiums von Leibniz' Schriften und im Vergleich mit den erhaltenen Rechenmaschinen fast zwingend nachvollziehen, dass die jetzt konstruierte und gebaute Maschine Leibniz' Vorstellungen entspricht.

Die Chiffrier-/Dechiffriermaschine „Machina Deciphratoria“ nach G.W. Leibniz

Wie die leibnizsche dezimale Vier-Spezies-Rechenmaschine enthält auch die in seinen Aufzeichnungen und Briefen – mit den Erfahrungen aus den Rechenmaschinen – beschriebene Chiffrier-/Dechiffriermaschine eine Staffelwalze als wichtiges Bauteil (Bilder 2 und 5).
Durch das Drücken einer Buchstabentaste (Leibniz schreibt: „*wie auf einem claviocord*“) wird die Transporttrommel um 60° gedreht (Bild 6). Auf deren Welle befindet sich die Staffelwalze mit sechs möglichen axialen Stellungen, welche die parallel nach vorne versetzte Anzeigetrommel mit den Buchstabenstreifen (mit den Buchstaben des Alphabetes) auf ihrer Peripherie um 60° weiterdreht. Je nach der axialen Stellung der Staffelwalze werden alle oder weniger Buchstaben auf die Anzeigetrommel kodiert. Zusätzlich werden einzelne Zähne der Staffelwalze weggelassen, wodurch eine wesentlich größere Zahl von Chiffrierungen möglich ist. Mit insgesamt sechs schwarzen Buchstabenstreifen des Alphabets und den sechs möglichen axialen Stellungen der Staffelwalze sowie fehlenden Zähnen gibt es also eine große Zahl von möglichen Verschlüsselungen (Bild 7). Entsprechendes gilt für die Entschlüsselung eines Textes mit sechs roten Buchstabenstreifen auf der Peripherie der Anzeigetrommel.

Der Verschlüsselungscode der hier verwendeten symmetrischen Substitutionsmethode besteht damit aus der Staffelwalze und den Buchstabenstreifen. Sender und Empfänger müssen diese besitzen, um zu ver- und entschlüsseln.

Der Vergleich dieser Chiffriermaschine mit der seit den 1920er Jahren entwickelten und im Zweiten Weltkrieg verwendeten, bedeutenden elektromechanischen Enigma lässt erkennen, welch hohen Verschlüsselungsgrad die leibnizsche Maschine bereits vor etwa 300 Jahren besaß.

Technische Vorgeschichte: Nachbauten der leibnizschen Rechenmaschine

Bekanntlich ist die erhaltene große leibnizsche dezimale Vier-Spezies-Rechenmaschine durch ihre empfindliche Konstruktionsweise und viele Schäden bei Reparaturversuchen leider nicht funktionsfähig.

Anhand unserer jahrzehntelangen konstruktiven und mathematischen Forschung, unterstützt durch ein DFG-Projekt, konnten wir die Probleme der Getriebekinematik dieser Rechenmaschine aus den

Jahren 1692-98 (Bilder 1 und 2) vollständig entschlüsseln und ein möglichst authentisches Funktionsmodell der leibnizschen Maschine (Bild 3) mit wichtigen kleinen Änderungen bauen. Auch großmaßstäbliche Funktionsmodelle wichtiger Bauteile wurden angefertigt und gehören zu unserer Leibniz-Dauerausstellung. Die Lösung des großen Problems der leibnizschen Rechenmaschine, nämlich vollständige Zehnerüberträge zu verwirklichen, wurde von Herrn Ing. (grad.) Klaus Badur, Garbsen, sowie von uns auf zwei verschiedene Weisen erreicht.

Seit 2005 haben wir auch zwei binäre Rechenmaschinen nach Leibniz gebaut: eine von Leibniz beschriebene Maschine mit abrollenden Kugeln auf einer zweifach schiefen Ebene in das Rechenwerk mit den erforderlichen Zweierüberträgen bei Addition und Multiplikation, sowie eine binäre Vier-Spezies-Getriebe-Rechenmaschine nach dem Vorbild der dezimalen Maschine – mit nur drei geänderten Zahnrädern pro Stelle einer Zahl im Vergleich hierzu. Dies ist die Folge der logisch und konstruktiv genialen, jedoch technisch aufwändigen und Toleranz-empfindlichen leibnizschen Bauweise.

Die Kryptographie

Seit dem Altertum ist die Kryptographie zunehmend in vielen Bereichen des praktischen Lebens und der Wissenschaft von großer Bedeutung. Heutzutage ist die elektronische Kryptographie ein weltweit gestaltendes und zugleich problematisches Hilfsmittel der Informations- und Kommunikationsgesellschaft. Das allgemeine öffentliche Interesse für Leibniz' Maschine, als einem sehr frühen Prototyp für mechanische Verschlüsselungen, dürfte damit sicher sein.

Die Kryptographie wurde bereits in den alten Kulturen im Nahen Osten und in den Ländern um das Mittelmeer entwickelt und auch von römischen Feldherren verwendet, z.B. mit Hilfe von Pergamentstreifen, die um Holzstäbe gewickelt wurden, oder Papierstreifen mit darunter liegenden verschiebbaren Buchstaben. In England gilt John Wallis im 17. Jahrhundert als der Vater der Kryptographie, mit dem Leibniz korrespondierte.

Vorgeschichte des Baus der Chiffriermaschine

Von Herrn Badur erhielten wir im vergangenen Jahr die Nachricht über die bedeutenden Forschungsergebnisse von Professor Nicholas Rescher von der Universität Pittsburgh, PA, USA, zu Leibniz' Vorschlägen für den Bau einer Chiffrier- und Dechiffriermaschine, auch mit konstruktiven Details, z.B. in vorbereitenden Notizen für seine Audienz bei Kaiser Leopold I. in Wien im Jahr 1688. Angeregt zur intensiven Beschäftigung mit Leibniz' jahrzehntelanger Befassung mit der Kryptographie wurde Professor Rescher u. a. durch die Studien von Professor Herbert Breger, bis vor wenigen Jahren Leiter des Leibniz-Archivs Hannover. Nach längeren Vorarbeiten entwarf Prof. Rescher, unterstützt durch den Ingenieur Richard Kotler, in den Jahren 2010 und 2011 aus den leibnizschen Vorschlägen die „*Machina Deciphratoria*", eine mechanische Chiffrier- und Dechiffriermaschine. Die modifizierte Konstruktion und die wichtigen Detailkonstruktionen übernahm Herr Badur, und gebaut wurde die Maschine von der Firma G. Rottstedt in Garbsen (Bilder 4 bis 7). Es ist hervorzuheben, dass Herr Badur nur durch seine eingehenden Studien und Kenntnisse, die er beim fast authentischen Nachbau der leibnizschen Vier-Spezies-Rechenmaschine erwarb, imstande war, zusammen mit der Firma Rottstedt ein handwerkliches Kunstwerk zu schaffen, das gestalterisch sehr gut dem Stil der Barock-Zeit nachempfunden ist.

Die Maschine wird von der Fritz Behrens Stiftung, Hannover, erworben und der Leibniz Universität Hannover als Dauerleihgabe zur Verfügung gestellt.

Herr Prof. Rescher war sehr daran interessiert, dass die Chiffrier-/Dechiffriermaschine ein Teil unserer Leibniz-Dauerausstellung wird, weil sie unseren Schwerpunkt der leibnizschen Erfindungen von Rechenmaschinen hervorragend vervollständigt.

Zur Begründung sei u. a. auf eine Passage des Briefes von Leibniz an Herzog Ernst August von Hannover aus den Jahren 1685-87 in französischer Sprache, ins Deutsche übersetzt, hingewiesen: „*Ich machte nicht viel Aufhebens von einzelnen Entdeckungen; was ich am nachdrücklichsten erstrebe, ist die Vervollkommnung der Erfindungskunst im Allgemeinen. Wichtiger als Lösungen von Problemen sind mir Methoden, denn eine einzelne Methode umfasst eine unendliche Zahl von Lösungen.*"
Leibniz war demnach in seiner *Ars inveniendi* (der Kunst des Erfindens) nicht an einzelnen technischen Erfindungen interessiert, sondern an ganzen Produkt-Systemen, die gemeinsame wichtige Bauteile enthielten. Ein solches ist die Staffelwalze (oder Stufenzahnrad), ein Zahnrad mit linear abnehmenden Zahnlängen; sie ist zunächst ein wichtiges Bauteil für die Zahleneingabe in der Rechenmaschine (die gesamte Länge für die Ziffer 1 und die kürzeste für die Ziffer 9).
Auch in der Chiffrier-/Dechiffriermaschine verwendete Prof. Rescher sehr naheliegend die Staffelwalze für die selektive Übertragung der Kodierungen von den Buchstabenstreifen auf die Anzeigetrommel; sie ist damit, gemeinsam mit dem Buchstabenstreifen und der Art der Substitution (z.B. Sprünge um zwei Buchstaben), der Schlüssel der Kodierung. Da die Staffelwalze in sechs möglichen axialen Positionen einstellbar ist, ergeben sich insgesamt viele Tausend Kodier-Möglichkeiten.
Es sei erwähnt, dass Leibniz das Prinzip der Staffelwalze (des Stufenzahnrades) nicht erfunden hat. In französischen Kirchturmuhren wurden zur Zeit von Leibniz Stufenscheiben für die Steuerung der Stundengeläute verwendet, und diese wurden auch in Taschenuhren für Repetier-Stundenschläge zur Zeitangabe eingebaut.

Zur Person: Erwin Stein

Emeritierter Professor für Baumechanik und Numerische Mechanik der Leibniz Universität Hannover. Im Jahr 1990 Konzipierung und Verwirklichung der ersten großen Leibniz-Wanderausstellung im Lichthof unserer Universität, nach langjährigen Studien über das leibnizsche Werk zusammen mit vielen Mitstreitern, mit dem Titel: „Gottfried Wilhelm Leibniz – seiner Zeit weit voraus – als Philosoph, Mathematiker, Physiker, Techniker…". Die Idee dieser Ausstellung war und ist, „Leibniz zum Anfassen und Begreifen" vorzustellen.

In den Jahren 2000 (anlässlich der Expo 2000 in Hannover, wiederum im Lichthof der Universität) und 2006 (in der Orangerie der Herrenhäuser Gärten) folgten zwei große Ausstellungen. Bis heute wurden acht weitere Ausstellungen in Deutschland und in der Österreichischen Akademie der Wissenschaften in Wien gezeigt; die bisher Letzte fand auf Einladung der Ruprecht-Karls-Universität Heidelberg im Jahr 2011 in der Heiliggeistkirche zu Heidelberg anlässlich der Gründung der Universität vor 625 Jahren statt.
Dann erfolgte in den Jahren 2008 und 2011 die Leibniz-Dauerausstellung in zwei Glaspavillons im Sockelgeschoss des Hauptgebäudes der Universität (des Welfenschlosses). Hierin befinden sich Bild- und Texttafeln sowie viele von uns gebaute Funktionsmodelle zu den Themen: Vita, Denkmaximen, Wissenschaftstheorie, Mathematik, Naturwissenschaften, technisch-mathematische Erfindungen (insbesondere dezimale und binäre Rechenmaschinen als Schwerpunkt der Ausstellung sowie Erfindungen für den Oberharzer Bergbau und die Wasserkünste der Herrenhäuser Gärten), Philosophie, Theologie, Sprach-, Geschichts-, Rechts-, Kunst-, Versicherungs- und Politikwissenschaften sowie Akademie-Gründungen.

Literatur

1. N. Rescher, Leibniz and Cryptography, University of Pittsburgh, PA, 2nd edition 2013
2. K. Badur, Konstruktionsbeschreibung und Videofilm der neuen Chiffriermaschine nach Leibniz (2013)
3. H. Breger, Leibniz und die Kryptographie, in: H. Breger, J. Herbst und S. Erdner (Hrsg.), Einheit in der Vielheit, Akten des VIII. Int. Leibniz-Kongresses, Hannover (2006), S. 101-105
4. E. Stein und F. O. Kopp, Konstruktion und Theorie der Leibnizschen Rechenmaschinen im Kontext der Vorläufer, Weiterentwicklungen und Nachbauten, mit einem Überblick zur Geschichte der Zahlensysteme und Rechenhilfsmittel, in: H. Breger et al. (Hg.), Studia Leibnitiana, Zeitschrift für Geschichte der Philosophie und der Wissenschaften, Band 42, Heft 1, erschienen in März 2012, Franz Steiner Verlag, Stuttgart (2010), 128 p.
5. A. Walsdorf, K. Badur, E. Stein, F.O. Kopp, Das letzte Original (die einzig erhaltene leibnizsche dezimale Vier-Spezies-Rechenmaschine), Gottfried-Wilhelm-Leibniz-Bibliothek (GWLB), Hannover (2014), 200 p.
6. E. Stein, Die Leibniz-Dauerausstellung der Gottfried Wilhelm Leibniz Universität, http://www.uni-hannover.de/de/universitaet/leibniz/leibnizausstellung/index.php (2008), p. 1-58
7. E. Stein und P. Wriggers (Hg.), Gottfried Wilhelm Leibniz – Philosoph, Mathematiker, Physiker, Techniker, Begleitbuch zur gleichnamigen Ausstellung, 2. Aufl., Leibniz Universität Hannover (2007)
8. K. Popp und E. Stein (Hg.), Gottfried Wilhelm Leibniz, Philosopher, Mathematician, Physicist, Engineer, Schlütersche/Universität Hannover (2000)

Hinweis:

Für weitere Informationen steht Ihnen Prof. Erwin Stein, Institut für Baumechanik und Numerische Mechanik der Leibniz Universität Hannover, Telefon +49 511 762 4290 oder E-Mail stein@ibnm.uni-hannover.de, gerne zur Verfügung.

Bilder zur leibnizschen Rechenmaschine und seiner vorgeschlagenen Chiffriermaschine

Bild 1: Originale ‚jüngere große' dezimale Vier-Spezies-Rechenmaschine, 8/16/1-stellig, gebaut von ca. 1692-98, Gottfried-Wilhelm-Leibniz-Bibliothek Hannover

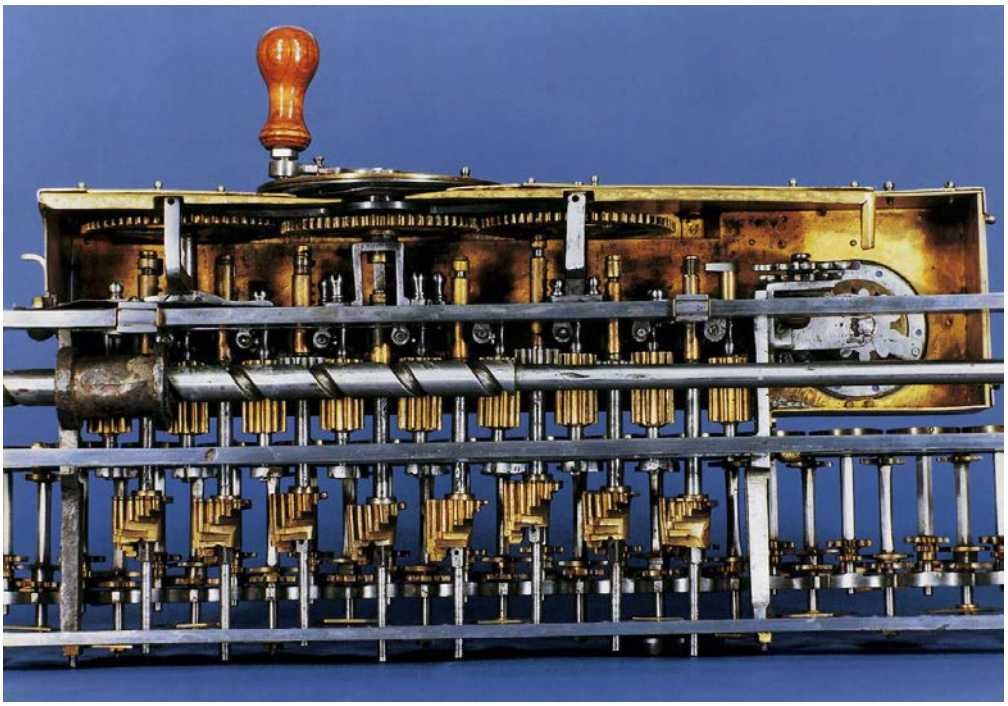

Bild 2: Originale ‚jüngere große' dezimale Vier-Spezies-Rechenmaschine, 8/16/1-stellig, Sicht von unten; die acht Staffelwalzen zur Zahleneingabe (mit verschieden langen Zähnen) sind deutlich zu erkennen.

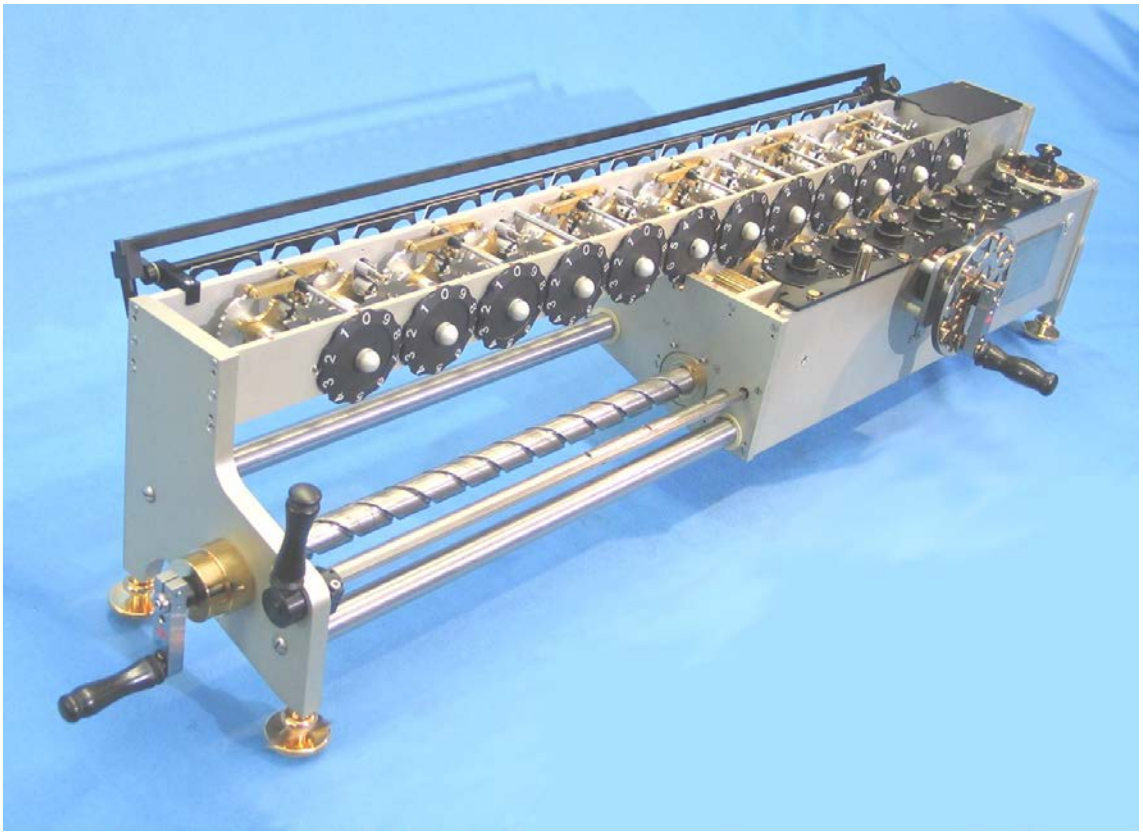

Bild 3: Hannoverscher Nachbau der leibnizschen dezimalen Vier-Spezies-Rechenmaschine mit Korrekturen für vollständige Zehnerüberträge und Optimierung der Getriebefunktionen, 6/12/1-stellig, K. Popp†, E. Stein, F.O. Kopp, 2005

Bild 4: Machina Deciphratoria (mechanische Chiffrier- und Dechiffriermaschine) nach G.W. Leibniz' Vorschlägen, ca. 1680-1700, Konstruktiver Entwurf von N. Rescher und R. Kotler, Detailkonstruktion von K. Badur, gebaut von G. Rottstedt, 2014

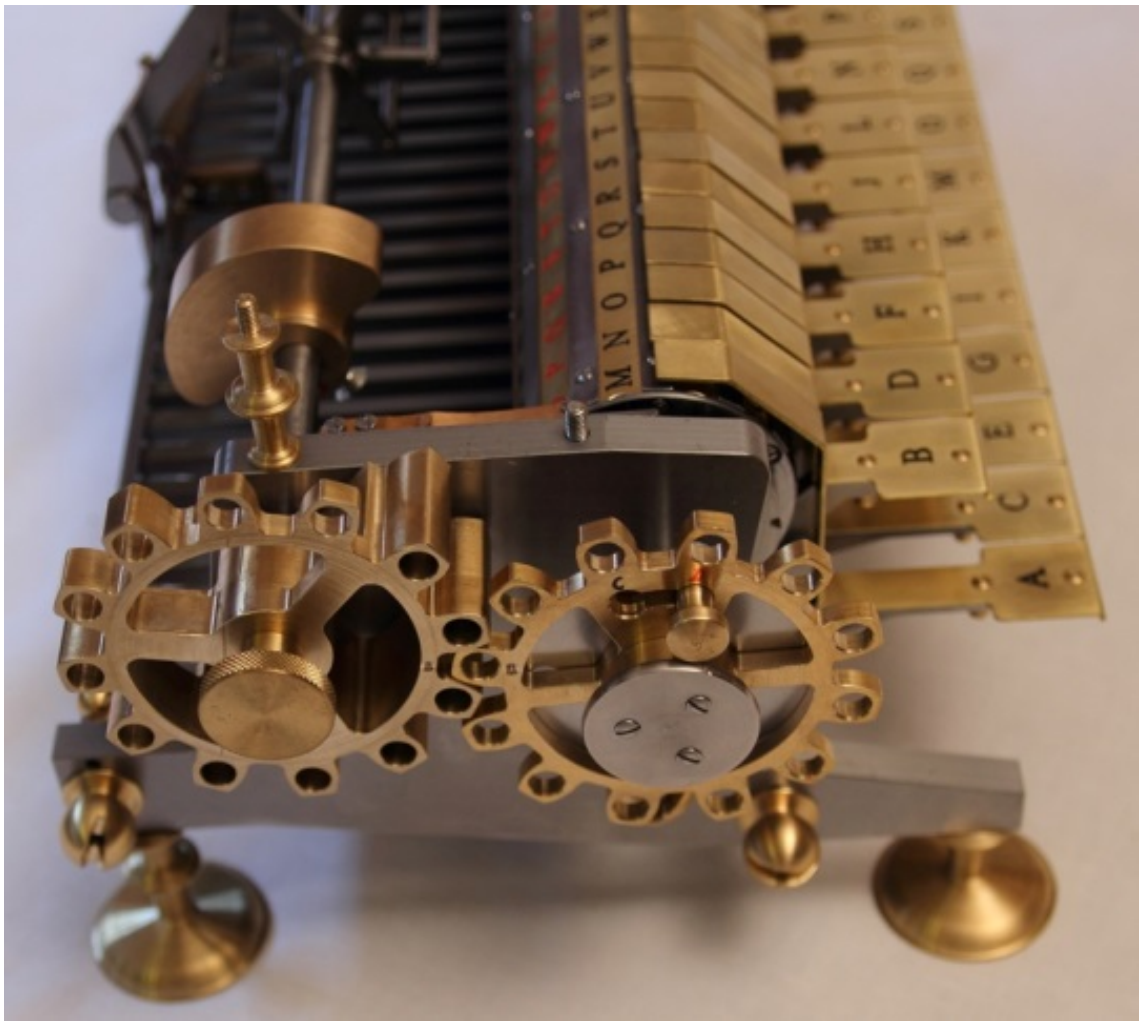

Bild 5: Machina Deciphratoria nach G.W. Leibniz' Vorschlägen, seitliche Ansicht mit Staffelwalze vor der Transporttrommel (links), Zahnrad der Anzeigetrommel (rechts) und Buchstabentasten

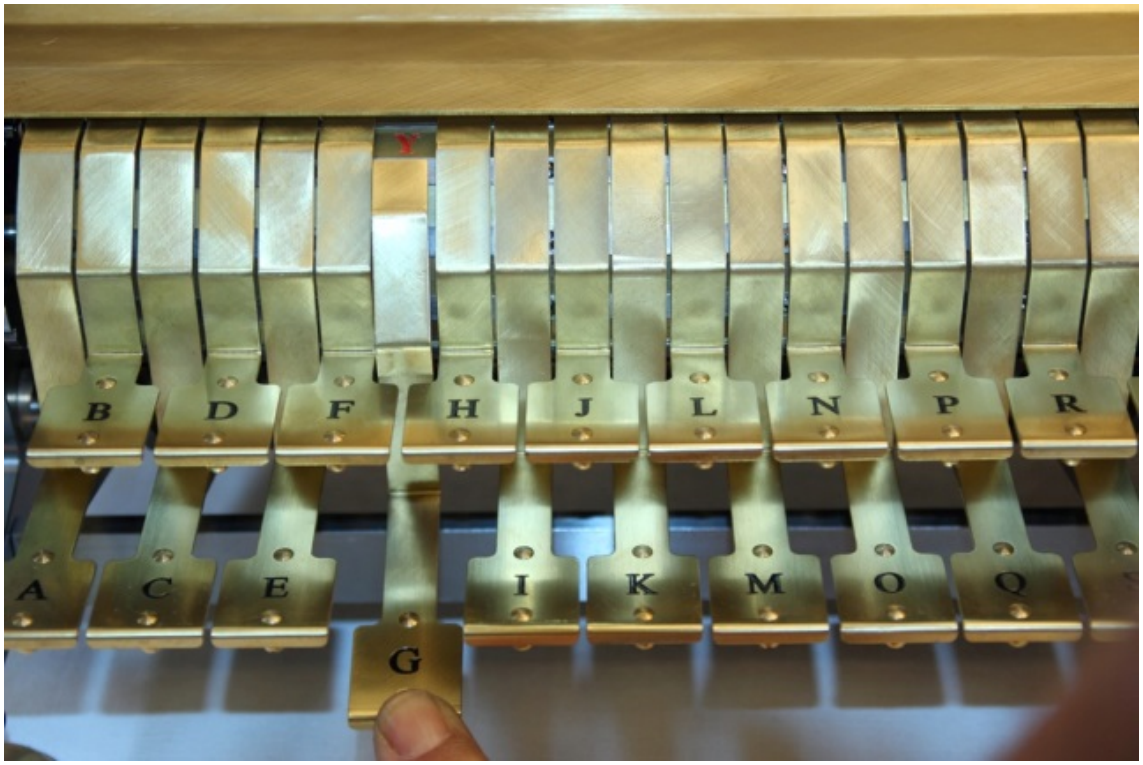

Bild 6: Machina Deciphratoria nach G.W. Leibniz' Vorschlägen, gedrückte Buchstabentaste G und entschlüsselter Buchstabe Y in der 4. Dekodierung

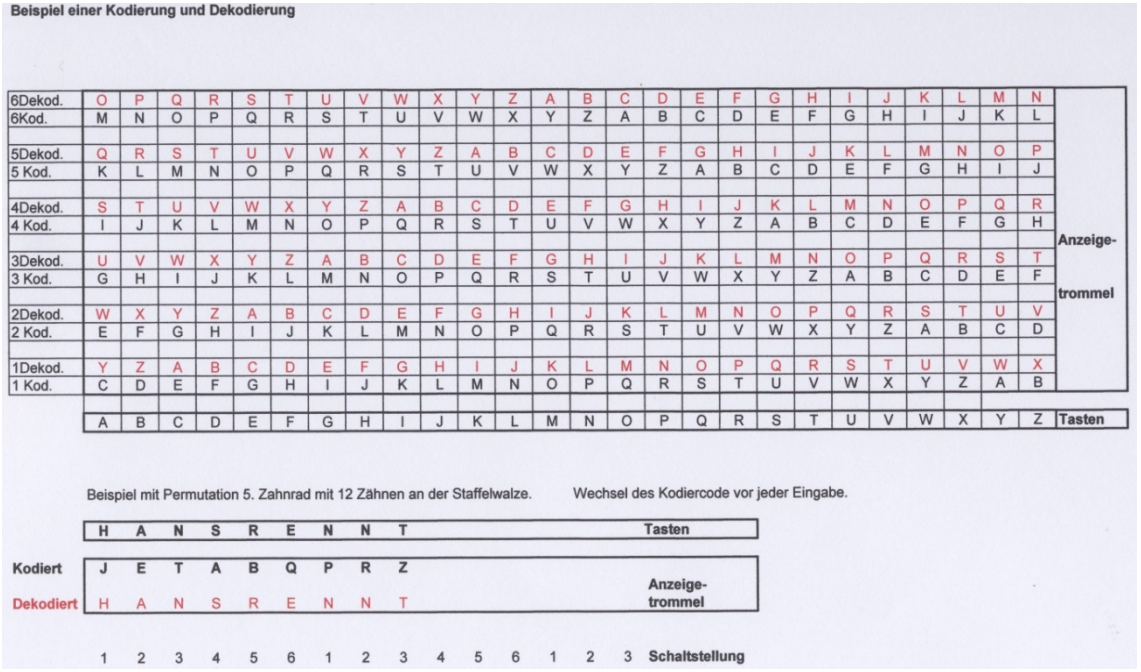

Bild 7: Zwei mal sechs Buchstabenstreifen mit dem Alphabet auf der Anzeigetrommel für jeweils sechs Kodierungen und Dekodierungen, hier mit jeweiliger Verschiebung um zwei Buchstaben