Universität Leipzig

Sommersemester 2017

Fakultät für Mathematik und Informatik

Modul: Aktuelle Trends der Informatik / VL + Übung Kryptographie

Dozent: Claus Diem

Autor: Maximilian Heinrich

Polyalphabetische Verschlüsselung in der frühen Neuzeit und die Machina Deciphratoria von Gottfried Wilhelm Leibniz

Inhaltsverzeichnis

1. Einleitung

Die Praxis des Chiffrierens von Nachrichten ist schon seit vielen Jahrhunderten bekannt, allerdings wurden bis zum Ende des I. Weltkriegs oftmals nur recht einfache monoalphabetische Verschlüsselungsverfahren verwendet. Sicherere polyalphabetische Verschlüsselungen hingegen waren zwar schon seit der Renaissance bekannt, konnten sich aber nicht durchsetzen, weil sie sich als zu kompliziert und fehleranfällig erwiesen. Diese Ausarbeitung will sich zunächst einen kurzen Überblick über die Geschichte der Kryptographie in der frühen Neuzeit (Frühmoderne) verschaffen. Mit diesem Vorwissen können im Anschluss die kryptographischen Leistungen von Gottfried Wilhelm Leibniz besser herausgearbeitet werden. Jüngere wissenschaftliche Publikationen zeigen, dass dieser auch auf dem Feld der Kryptographie herausragende Verdienste erzielte, indem er eine mechanische Chiffriermaschine, die Machina Deciphratoria, entwarf, gute 200 Jahre vor der eigentlichen Verwendung solcher Maschinen. Ziel dieser Ausarbeitung ist es einen Überblick über polyalphabetische Verschlüsselungen in der frühen Neuzeit/Frühmoderne und die kryptologischen Leistungen von Leibniz zu erhalten.

Im Vorfeld seien hier noch die wichtigsten Begriffe kurz erläutert: Im strengen Sinn bezeichnet Code das Festlegen von bestimmten Informationen. Dabei wird ein Wort bzw. ein Satz durch ein anderes Wort/Symbol/Satz ersetzt. Ein Beispiel dafür ist das Codewort mit dem man z.B. ganze Handlungsanweisungen abkürzt. Eine Chiffre hingegen arbeitet auf der Buchstabenebene. Hier wird jeder Buchstabe einer Nachricht durch einen anderen Buchstaben ersetzt.[1] Die monoalphabetische Verschlüsselung verwendet dabei nur ein einziges Substitutionsalphabet für den gesamten Nachrichtenraum; bei der polyalphabetischen Verschlüsselung hingegen wird das Substitutionsalphabet nach einem bestimmten Muster gewechselt. Des Weiteren werden die Begriffe kryptographisch bzw. kryptologisch in dieser Ausarbeitung synonym verwendet.

[1] Singh 2000: 12f.

2. Geschichte der Kryptographie in der frühen Neuzeit

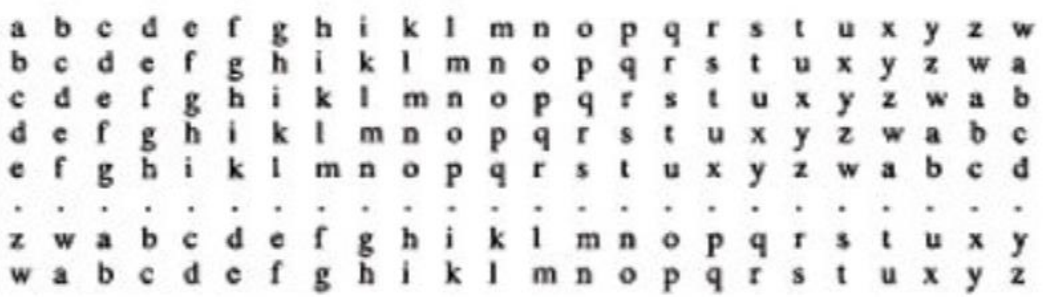
Als einer der ersten Europäer der Frühmoderne, der sich mit Kryptographie beschäftigte, gilt Leon Battista Alberti (1404─1472). Alberti, ein Universalgenie der Renaissance, hat maßgeblich die Verwendung von Chiffrierscheiben mitbegründet. Mag eine solche Chiffrierscheibe für sich allein genommen nur eine monoalphabetische Verschlüsselung darstellen, kann sie aber mit der richtigen Verwendungsweise für eine polyalphabetische Verschlüsselung genutzt werden. Beide Seiten vereinbaren dazu zunächst einen Indexbuchstaben. Dann gleicht der Verschlüssler diesen Buchstaben mit einem beliebigen Buchtstaben auf der äußeren Seite seiner Chiffrierscheibe ab. Der Buchstabe mit dem abgeglichen wurde, wird auf die Nachricht geschrieben. Nach drei, vier auf diese Weise verschlüsselten Wörtern findet ein Wechsel des Referenzbuchstabens statt, der mit dem vereinbarten Indexbuchstaben verglichen wird. Ein damit verbundener Wechsel des Chiffrieralphabets wird dann auch in der Nachricht vermerkt, beispielsweise indem ein Buchstabe größer geschrieben wird. Eine weitere kryptographische Erfindung von Alberti ist z.B. der doppelt verschlüsselte Code.[2] Allerdings hatten seine Erfindungen nicht den dynamischen Einfluss, den man mit dem heutigen Wissensstand von solchen Erfindungen erwarten sollte. John Addington Symonds fasst die Situation von Alberti treffend zusammen:

This man of many-sided genius came into the world too soon for the perfect exercise of his singular faculties. Whether we regard him from the point of view of art, of science, or of literature, he occupies in each department the position of precursor, pioneer, and indicator. Always original and always fertile, he prophesied of lands he was not privileged to enter, leaving the memory of dim and varied greatness rahter than any sold monument behind him.[3]

Ein weiterer Vertreter der Kryptographie in der frühen Neuzeit war Johannes von Trittenheim (1464─1516), besser bekannt unter seinem Pseudonym Trithemius, der sich ebenfalls der polyalphabetischen Verschlüsselung widmete. Erstmals wird hier mit einer sogenannten Tabula Recta, einer Verschlüsselungstabelle, gearbeitet bei der die einzelnen Alphabete systematisch ineinander verschoben werden (Shift). Der Vorteil gegenüber Alberti besteht darin, dass das Alphabet nach jedem Buchstaben gewechselt wird und nicht wortweise. Der Nachteil liegt allerdings darin, dass man jede Tabellenzeile einzeln hintereinander zur Verschlüsselung

[2] Kahn 1996: 128ff.
[3] Symonds 1927: 159

verwendet; es gibt kein Schlüsselwort um die Reihenfolge der einzelnen Verschlüsselungs-alphabete festzulegen.[4]



(Abbildung 1: Eine Tabula Recta, nach Trithemius[5])

Eine Weiterentwicklung in der polyalphabetischen Verschlüsselung fand durch Giovan Battista Bellaso (1505─≈1581) statt. In seinem 1553 erschienenen Buch „La cifra del. Sig. Giovan Battista Bellaso“ schlug er die Verwendung eines Bestätigungszeichens vor, um unterschiedliche Verschlüsselungen zu erhalten. Es gibt damit erstmals ein Schlüsselwort bzw. einen Schlüsselsatz, der die Reihenfolge der entsprechenden Verschlüsselungsalphabete festlegt. Für die einzelnen Chiffrieralphabete verwendete Ballaso, wie Trithemius, Standardalphabete, im Sinne der Tabula Recta, die sich nur marginal voneinander unterschieden.[6] Ebenfalls in diesem Zusammenhang ist der Name Giovanni Battista della Porta (1535─1615) zu nennen. Dieser mischte die Ideen von Alberti, Trithemius und Bellaso und veröffentlichte 1563 „De Furtivis Literarum Notis.“ Dabei deutet Porta bereits die Möglichkeit an die Verschlüsselungsalphabete beliebig festzulegen und nicht dem strengen Shift-Muster der Tabula Recta zu folgen, formuliert seine Beispiele allerdings nur mit der bekannten Tabula Recta.[7] Als Haupterfinder der polyalphabetischen Verschlüsselung gilt heute gemeinhin Blaise de Vigenère (1523─1596), wobei sich das ‚de‘ in seinem Namen im Übrigen nur darauf bezieht, dass er aus der gleichnamigen Stadt Vigenère stammt; er hatte keinen adligen Vorfahren. 1586 erschien sein Werk „Traicté des Chiffres“. Interessanterweise folgt die Erfindung, die heutzutage hauptsächlich mit den Namen Vigenère verbunden wird, der Technik von Bellaso; es gibt ein Standardalphabet, eine Tabula Recta und ein Schlüsselwort.[8] Dabei hat Vigenère auch explizit andere Verschlüsselungstechniken, wie z.B. den Autokey entwickelt, wo der zuvor entzifferte Klartext als neuer Schlüssel für die weitere Entzifferung der Nachricht dient.

[4] Kahn 1996 135ff.
[5] Kahn 1996: 136
[6] Kahn 1996 137
[7] Kahn 1996: 141f.
[8] Kahn 1996: 147ff.

Diese Verdienste von ihm sind aber im Laufe der Geschichte in Vergessenheit geraten. Die durch seinen Namen geprägte Vigenère-Verschlüsselung galt lange Zeit als unknackbar bzw. als „Le Chiffre Indéchiffrable“, obwohl schon durch Porta geeignete Angriffsmöglichkeiten entwickelt wurden. Wären die Schriften von Porta populärer gewesen, hätte diese Art der Verschlüsselung niemals ihren legendären Ruf erhalten. Offiziell wurde die Vigenère-Verschlüsselung erst Mitte des 19. Jahrhunderts entschlüsselt, was aber auch ein so renommiertes Magazin wie den Scientific American nicht daran hinderte, diese noch 1918(!) als unknackbar zu betiteln.[9]

Auch in den Zeiten der Frühmoderne bestand bereits ein starkes Bedürfnis nach Verschlüsselung. Diplomatie und Politik kommunizierten in der damaligen Zeit hauptsächlich auf dem Postweg miteinander, womit das Risiko bestand, dass die Informationen zwischendurch in unbefugte Hände gerieten. Der Ausweg aus diesem Dilemma lag in der Verschlüsselung der Kommunikation. Gleichzeitig wusste man natürlich über den Umstand und war von staatlicher Seite aus daran interessiert die vertrauliche Kommunikation anderer Staaten mitlesen zu können. In der Zeit um 1700 hatte daher so gut wie jeder europäische Fürstenhof seine eigene nachrichtendienstliche Abteilung, die als Schwarze Kammern bezeichnet wurden. Durch diese wurden Nachrichten systematisch abgefangen, Abschriften abgefertigt und verschlüsselte Botschaften dechiffriert.

In diesem Kontext besonders hervorzuheben ist die Schwarze Kammer in Wien, auch bekannt als „Geheime Kabinettskanzlei“, die sich durch eine schier unglaubliche Effektivität auszeichnete und als die beste in Europa galt. Der Prozess des Abfangens, Öffnens, Entschlüsselns und Weiterleitens von Nachrichten war systematisch und detailliert geregelt. So wurde Post, die am selben Tag den ortsansässigen Botschaften zugestellt werden sollte, gegen 07:00 Uhr zur Schwarzen Kammer gebracht und war bereits 09:30 Uhr auf dem Weg zurück zum Hauptpostamt, um die planmäßige Zustellung nicht zu gefährden. Post auf dem Transitweg kam um 11:00 Uhr herein und wurde gegen 14:00 Uhr wieder in den regulären Postweg zurückgeleitet. Nachrichten, die an dem Tag in die Post aufgegeben waren, wurden um 16:00 Uhr zu den Spezialisten der Schwarzen Kammer gebracht und waren um 18:30 Uhr wieder auf dem Weg zu ihrer ursprünglichen Bestimmung.[10]

In der Zwischenzeit wurden die einzelnen Korrespondenzen feinsäuberlich geöffnet, die Reihenfolge des Inhalts festgehalten und Abschriften der relevanten Inhalte angefertigt. Zuletzt

[9] Kahn 1996: 148
[10] Kahn 1996: 163ff.

wurden die Briefe mit gefälschten Siegeln wieder verschlossen. Um eine schnelle Kopie der Briefe vornehmen zu können, standen entsprechende Stenographen bereit. Längere Korrespondenzen wurden diktiert bzw. waren gleichzeitig bis zu vier Stenographen mit einer Abschrift beschäftigt. Danach wurden die einzelnen verschlüsselten Botschaften zu den Kryptoanalysten der Schwarzen Kammer gebracht, die mit der Entschlüsselung begannen. Auch die Ausbildung bzw. Arbeitsweise der Kryptoanalysten ist für damalige Verhältnisse als höchst professionell zu beurteilen; so gab es einen Beschäftigungsrhythmus von einer Woche Arbeit mit einer darauffolgenden Woche Urlaub und für erfolgreiche Entschlüsselungen wurden Prämien gezahlt. Wurde ein entsprechender Schlüssel für eine Nachricht anderwärtig beschafft, z.B. durch Spionage, gab es für die Kammermitarbeiter sogar eine Entschädigung, da ihre Leistungen für die damit verbundene Entschlüsselung nun nicht mehr benötigt wurden. Eingestellt wurden in der Regel junge Mitarbeiter Anfang 20 mit mathematischem Grundverständnis und Kenntnissen von Französisch und Italienisch, die systematisch ausgebildet wurden. Des Weiteren standen für fremdsprachige Nachrichten auch Übersetzer zur Verfügung. Wurde eine Sprache, wie z.B. Armenisch, nicht beherrscht, wurden dafür benötigte Experten rekrutiert. Insgesamt arbeiteten ungefähr 10 Mann in der Geheimen Kabinettskanzlei in Wien, die zwischen 80 und 100 Briefen am Tag abfingen.[11] Es ist dabei anzumerken, dass die meisten Nachrichten relativ leicht zu entziffern waren, da überwiegend monoalphabetische Verschlüsselungsmethoden verwendet wurden.

3. Fehleranfälligkeit der monoalphabetischen Verschlüsselung

Wenn eine solche Überwachungspraxis des Nachrichtenverkehrs schon im 18. Jahrhundert üblich war und auch alle beteiligten Seiten davon wussten, dass dies der Fall ist, stellt sich die Frage, warum dann nicht konsequent sichere polyalphabetische Verschlüsselungen angewendet wurden, deren Grundzüge in der damaligen Zeit durch die Publikationen von Alberti, Trithemius, Porta und Vigenère mehr oder weniger bekannt waren. Der Grund dafür lag hauptsächlich in ihrer Kompliziertheit. Zwar ist eine polyalphabetische Verschlüsselung sicherer, doch ist das dabei verwendete Verschlüsselungsverfahren auch hochgradig fehleranfällig. Wenn das Chiffrieralphabet bei jedem Buchstaben wechselt, kann schon ein einzelner unlesbarer Buchstabe bzw. ein unleserliches Wort ausreichen, um eine ganze Nachricht unleserlich werden zu lassen. Die offiziellen Nachrichtenempfänger bzw. Sekretäre

[11] Kahn 1996: 163ff.

außerhalb der Schwarzen Kammern waren keine hauptamtlichen Kryptoanalytiker, die über die nötigen Kenntnisse verfügten mit solchen Fehlern bzw. Schwierigkeiten umgehen zu können. Ebenfalls hatten sie noch eine Vielzahl anderer Aufgaben zu erledigen. Wenn also eine Nachricht für sie nicht zu entschlüsseln war, wurden keinen weiteren Dechiffrierversuche unternommen; stattdessen musste der Absender informiert werden seine Nachricht ein weiteres Mal, in leserlicherer Form, zu versenden.[12] Eine komplizierte Form der Verschlüsselung konnte also dazu führen, dass die Kommunikation stark erschwert wurde, weswegen man für eine verlässliche Form der Verständigung eher auf die bewährten monoalphabetischen Verschlüsslungen zurückgriff. So berichtet ein ehemaliger Botschafter von Ludwig dem XIV., François de Callières, dass Sicherheit im Nachrichtenverkehr durch eine unendliche Anzahl an verschiedenen Schlüsseln erlangt werden kann, die auf einem allgemeinen Modell basieren. Diese Chiffren, so Callières, die von Professoren in Universitäten erdacht werden und algebraischen bzw. arithmetischen Regeln unterliegen sind aber unpraktisch aufgrund ihrer großen Länge und den Schwierigkeiten bei ihrem Gebrauch; gewöhnliche Chiffren dagegen werden fast so schnell wie normale Briefe niedergeschrieben.[13] Dieser Umstand mag naheliegen, denn ist man einmal mit einer monoalphabetischen Verschlüsselung vertraut, muss man nur für jeden Buchstaben ein entsprechendes Pendant kennen. Dies vereinfacht die praktische Handhabung ungemein, wenn man bedenkt, dass beispielsweise eine Diplomatische Vertretung in der damaligen Zeit pro Tag dutzende Botschaften sendete und empfing. Selbiges gilt für den militärischen Nachrichtenverkehr, der schnell und einfach erfolgen muss.[14] Wenn also das größte Problem bei der polyalphabetischen Verschlüsselung der menschliche Faktor ist, dann wäre eine automatisierte Form der Ver- und Entschlüsselung die ideale Lösung, um solchen Problemen begegnen zu können und damit die Fehleranfälligkeit durch den menschlichen Faktor auszuschließen. Dieser Gedanke führt geradewegs zu der revolutionären Idee einer mechanischen Chiffriermaschine.

[12] Kahn 1996: 150/151
[13] Kahn 1996: 150
[14] Singh 2000: 73

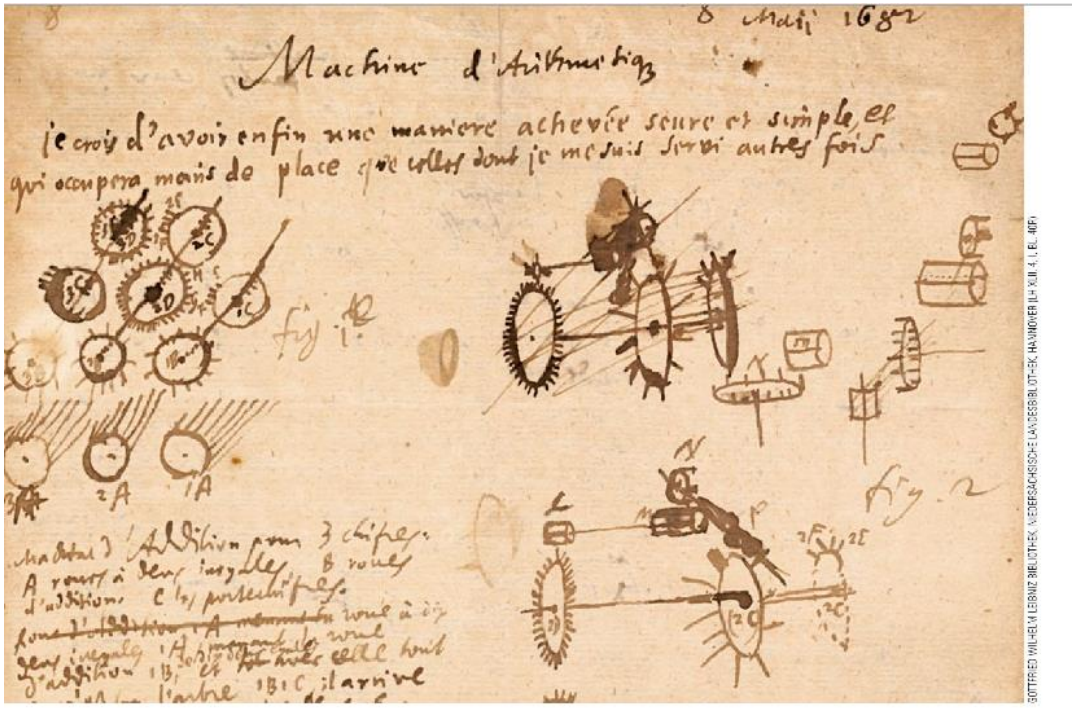
4. Die Machina Deciphratoria von Leibniz

Gottfried Wilhelm Leibniz (1546–1616), ein Universalgenie des 17. Jahrhunderts, gilt gemeinhin als deutscher Leonardo da Vinci, auch wenn er sich tendenziell mehr mit mathematischen und ideellen Themengebieten beschäftigte und weniger mit Kunst, wie sein italienischer Kollege. Die revolutionäre Idee von Leibniz auf dem Gebiet der Kryptographie besteht in nichts Geringerem als in der Entwicklung einer „Proto-Enigma", einer mechanischen „Rotor-Chiffriermaschine", bei der das verwendete Chiffrieralphabet bei den einzelnen Buchstaben automatisch gewechselt wird, was die Langsamkeit und Fehleranfälligkeit bei der polyalphabetischen Verschlüsselung minimiert.

Dass die Maschine in der Forschungsliteratur erst etwa seit den letzten 10 Jahren Erwähnung findet, liegt daran, dass sie, ebenso wie die berühmte mechanische Rechenmaschine von Leibniz, zu dessen Lebzeiten nie gebaut wurde. Aus den über 100.000 Seiten seines gesamten Nachlasses lässt sich allerdings das grundlegende Funktionsprinzip der Maschine rekonstruieren. Was aber auch festzuhalten ist, genauso wie seine mechanische Rechenmaschine, die Machina Arithmetica, hätte auch seine entworfene Chiffriermaschine, die Machina Deciphratoria, funktioniert. Der Hauptgrund für das Nicht-Bauen seiner Rechenmaschine lag damals nicht in ihrer mangelnden theoretischen Ausgereiftheit, sondern darin, dass die dazu benötigten Bauteile damals noch nicht in der erforderlichen Präzision gefertigt werden konnten. So müssen für eine erfolgreiche Realisierung an insgesamt 1650 Zahnflankenpaarungen die Maße auf die hundertstel Millimeter genau eingehalten werden und außerdem darf dabei die Orientierung der einzelnen Wellen höchstens um 0,1 Grad von der exakten Position abweichen, weswegen es nicht verwundert, dass die Maschine damals nicht gebaut werden konnte.[15] Im Gegensatz dazu hätte die Chiffriermaschine von Leibniz aber zur damaligen Zeit durchaus realisiert werden können, da der technische Aufwand hierzu bedeutend geringer ausgefallen wäre, allerdings erkannte niemand ihr Potential.

Es ist anzumerken, dass Leibniz ein revolutionärer Ideengeber war, aber kein Praktiker. So gab er bei seiner Rechenmaschine nur grobe Skizzen vor (siehe Abbildung 2) und erwartete, dass die beauftragten Konstrukteure die Arbeit entsprechend so ausführen, wie es gemäß seiner theoretischen Vorstellung sein sollte, was bei der konkreten Realisierung immer wieder zu Schwierigkeiten führte.[16]

[15] Badur 2016: 80
[16] Badur 2016: 79f.



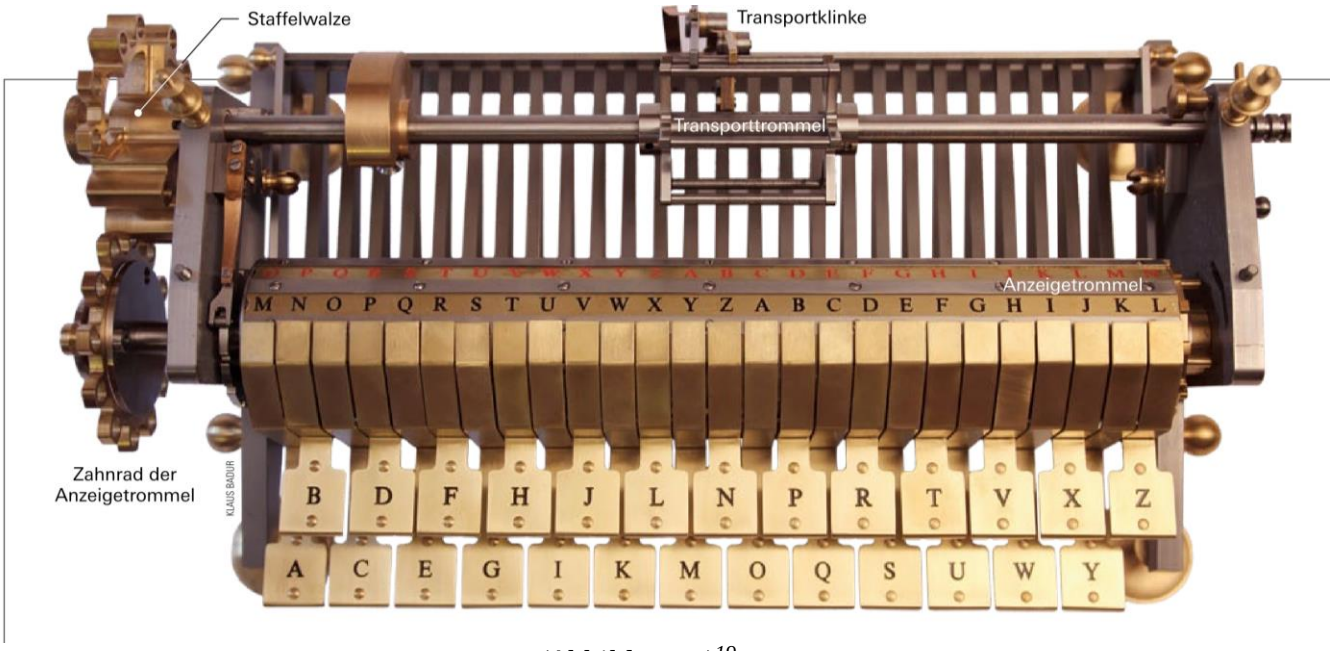
(Abbildung 2)[17]

Selbiges gilt für die Chiffriermaschine von Leibniz; die hier folgende Vorstellung seiner Maschine beruht daher auf verschiedenen Aufzeichnungen in seinem Nachlass und es ist durchaus vorstellbar, dass Leibniz bestimmte Details anders entworfen hätte. Eine entsprechende Rekonstruktion der hier vorgestellten Kryptographiemaschine wurde von Nicolas Rescher entworfen und die Zusammensetzung mit Richard Kotler vorgenommen; die Detailkonstruktionen stammen dabei von Klaus Badur.[18]

4.1. Aufbau der Maschina Deciphratoria

Der Aufbau dieser Maschine ist relativ einfach (Abbildung 3), es gibt im Endeffekt eine Anzeigetrommel und eine Transporttrommel. Der Benutzer gibt auf einer klavierähnlichen Tastatur die zu verschlüsselnde Nachricht ein und für jeden Klartextbuchstaben wird ein entsprechender Chiffrierbuchstabe auf der Anzeigetrommel ersichtlich. Bisher entspricht dieses Verfahren genau einer monoalphabetischen Verschlüsselung, mit der Ausnahme, dass das Eingeben und Ablesen aufgrund der Tasteneingabe etwas komfortabler sein mag.

[17] Badur 2016: 80
[18] Stein 2014: 2



(Abbildung 3)[19]

Die technische Raffinesse der Leibniz-Maschine besteht darin, dass eine sogenannte Staffelwalze mit der Anzeigetrommel verbunden ist. Diese bewirkt nach einer gewissen Anzahl von eingegebenen Buchstaben eine Drehung der Anzeigetrommel um 60° und damit einen Wechsel des verwendeten Chiffrieralphabets, womit die verwendete Verschlüsselung polyalphabetisch wird.[20] Ist z.B. das Rotationsmuster 1 1 1 0 0 0 durch die Staffelwalze eingestellt, dann wechselt die Maschine folgendermaßen das Verschlüsselungsalphabet, wobei unterschiedliche Zahlen unterschiedliche Zustände bzw. Chiffrieralphabete kennzeichnen:

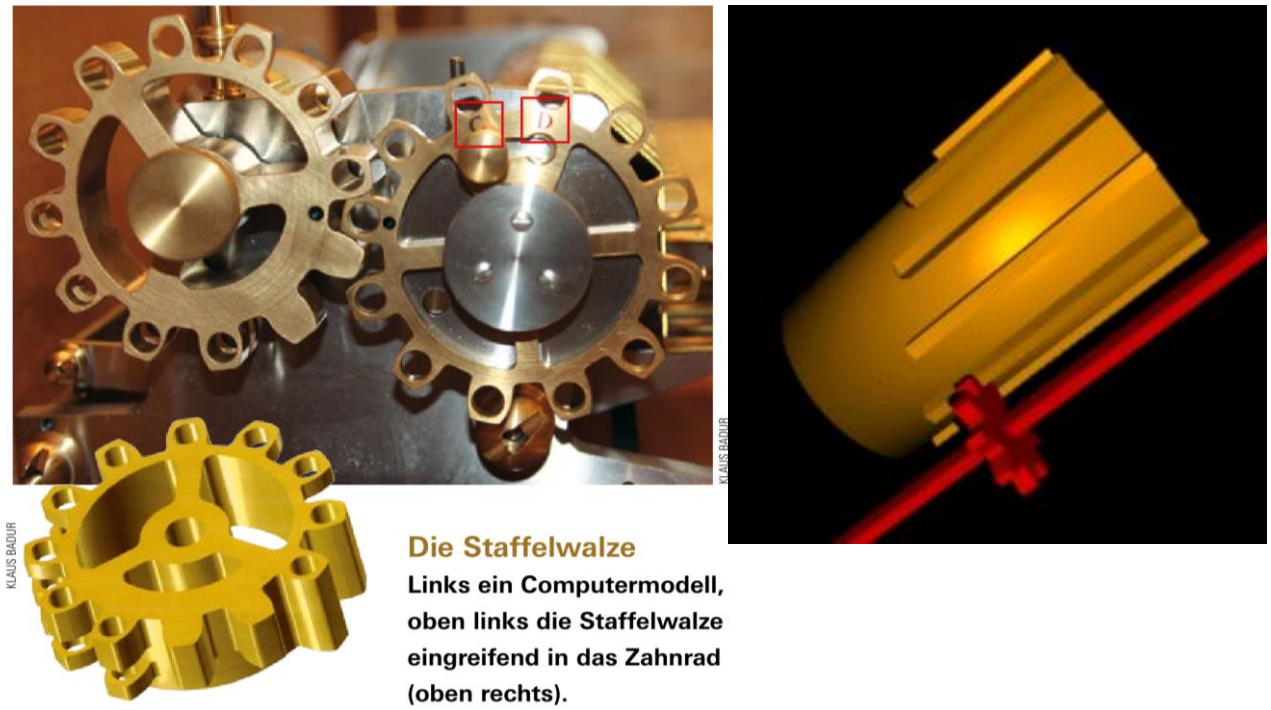
1 – 2 – 3 – 4 – 4– 4 – 4 – 5 – 6 – 1 – 1 – 1 – 1 – 2 – 3 – 4 etc.

Die Maschine beginnt im Zustand 1 mit dem entsprechenden Alphabet; die ersten drei Tasteneingaben führen jeweils zu einem Wechsel des Zustands bzw. des Chiffrieralphabets, bei den nächsten drei Eingaben geschieht nichts weiter, bis wieder das Alphabet dreimal hintereinander gewechselt wird. Da auf einer Anzeigetrommel 6 unterschiedliche Chiffrieralphabete vorhanden sind, wird nach sechs Umdrehungen je 60° wieder das zuerst verwendete Chiffrieralphabet erreicht, was hier den Wechsel von 6 auf 1 erklärt. Auf diese Weise entsteht ein zyklisches Muster. Es ist anzumerken, dass diese Festlegung auf 6 Alphabete eine willkürliche Festlegung bei der Rekonstruktion gewesen ist; Leibniz hätte ebenso gut mit einer Anzeigetrommel mit 10 Alphabeten arbeiten können.[21] Das Dechiffrieren einer verschlüsselten Nachricht geschieht ähnlich. Die Alphabete auf der Anzeigetrommel sind so

[19] Badur 2016: 86
[20] Rescher 2012: 40
[21] Rescher 2012: 89

gestaltet, dass unter einem verwendeten Chiffrieralphabet das jeweilige Klartextalphabet zu finden ist. Um eine Nachricht zu entschlüsseln kann die Maschine einfach auf das Klartextalphabet umgestellt werden und über die Tatstatur wird die verschlüsselte Botschaft eingegeben. Auf der Anzeigetrommel erscheint nun der Klartext.

Technisch wird der Wechsel des Alphabets also durch die Verwendung einer Staffelwalze ermöglicht, die einem unregelmäßigen Zahnrad ähnelt. Ihre grundlegende Funktionsweise wird durch folgende Abbildung verdeutlicht:



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

(Abbildung 4)[22]

Durch unterschiedliche und unregelmäßig angeordnete Keile auf der Staffelwalze stehen unterschiedliche Rotationsmöglichkeiten der Anzeigetrommel zur Verfügung. Obwohl die Staffelwalze manchmal auch als „Leibniz-Rad“ bezeichnet wird, stammt diese Erfindung aber nicht von Leibniz selbst und wurde z.B. schon vorher bei französischen Kirchturmuhren verwendet.[23] Die Maschine von Rescher/Kotler/Badur weist dabei folgende Drehmuster auf; eine 1 steht hierbei für eine Drehung um 60°:[24]

[22] Badur 2016: 87/ Wikipedia 2010
[23] Stein 2014: 3
[24] Rescher 2012: 39

1 0 0 0 0 0

1 1 0 0 0 0

1 1 1 0 0 0

1 1 1 1 0 0

1 1 1 1 1 0

1 1 1 1 1 1

Ein und dieselbe Staffelwalze kann also unterschiedliche Rotationsmuster ermöglichen. Wie Abbildung 4 zeigt sind die Keile („Zähne“) der Walze breiter, als es für eine direkte Übertragung erforderlich ist. Demnach kann die Walze seitlich verstellt werden, um auf diese Weise die verschiedenen Rotationsmuster zu ermöglichen. Wie ein Rotationsmuster genau erfolgt, ist dementsprechend auch von der genauen Starteinstellung der Staffelwalze abhängig.

Wie sieht es nun mit der Sicherheit einer solchen Maschine aus? Für den Fall, dass 50 Chiffrieralphabete insgesamt zur Verfügung stehen und auf einer Anzeigetrommel davon 6 Alphabete verwendet werden, gibt es (50! / 44!) = 11.441.304.000 unterschiedliche Verschlüsselungsmöglichkeiten, die durch eingelegte Alphabetleisten auf der Anzeigetrommel realisiert werden können. In Bezug auf die Rotationsmuster gibt es für die Konstruktion einer Staffelwalze insgesamt 2^6 = 64 verschiedene sequenzielle Muster.[25] Multipliziert ergeben diese beiden Zahlen damit mehrere hundert Milliarden Verschlüsselungsmöglichkeiten. Für den Fall, dass man die Sicherheit noch weiter erhöhen will, kann man einfach die Zahl der verwendeten Chiffrieralphabete bis auf $26! \approx 4{,}03 * 10^{26}$ erhöhen, falls man das deutsche Alphabet mit 26 Buchstaben verwendet und alle Möglichkeiten der Substitution ausschöpft. In der Praxis wäre eine solche Vielzahl an Verschlüsselungsmöglichkeiten aber wohl kaum verwirklicht worden; so schildert Rescher die plausible Möglichkeit, dass man einfach 6 zufällige Alphabetleisten, ausgewählt aus einer 10 * 10 Box von 100 Möglichkeiten, für die Anzeigetrommel verwenden könnte.[26] Angesichts der astronomisch hohen Zahl an Verschlüsselungsmöglichkeiten ist in der forschungsbasierten Literatur oftmals davon zu lesen, dass diese Maschine in Bezug auf die Sicherheit mit der Enigma mithalten konnte.[27] Bei solchen Feststellungen ist allerdings auch anzumerken, dass kryptographische Sicherheit nicht immer mit der bloßen Zahl der möglichen Verschlüsselungsmöglichkeiten beurteilt werden kann, denn nach dieser Argumentationsform

[25] Rescher 2012: 40 (Achtung: Schreibt von 2^5 = 64 [sic!] Möglichkeiten)
[26] Rescher 2012: 41
[27] Badur 2016: 87

bietet bereits eine einfache monoalphabetische Substitution gigantisch viele Möglichkeiten; wie gezeigt bietet das deutsche Alphabet insgesamt 26! Verschlüsselungsmöglichkeiten. Ein Kryptoanalyst probiert aber nicht stur alle Möglichkeiten durch, sondern schaut in dem Fall nach der jeweiligen Buchstabenhäufigkeit, was schnell zu Rückschlüssen auf die verwendeten Wörter führt.

In dieser Hinsicht ist auch das Verschlüsselungsverfahren der Machina Deciphratoria nicht unangreifbar. Kennt man das Rotationsmuster, dann weiß man, dass sich ein entsprechendes Verschlüsselungsalphabet alle n-Stellen wiederholt. Hier kann es theoretisch einen Angriff auf die polyalphabetische Substitution geben, wie er von Friedrich Kasiski und Charles Babbage erfunden wurde, bei dem man nach entsprechenden Bi- bzw. Trigrammen sucht, also entsprechenden Wiederholungen von Buchstabenpaaren innerhalb des Chiffriertextes. Ist auf diese Weise das Rotationsmuster durchschaut, dann liegt die Sicherheit vor allem in der konkret realisierten Art der Verschlüsselung. Bei Trithemius und der klassischen Vigenère-Verschlüsselung geschieht die Generierung der einzelnen Verschlüsselungsalphabete durch die Tabula Recta. Da dies im Endeffekt nur eine Verschiebung des gesamten Alphabets darstellt, bewirkt dies, dass man das ganze Verschlüsselungsalphabet für eine Verschlüsselungs-einstellung rekonstruieren kann, sobald man ein einziges Buchstabenpaar des verwendeten Alphabetes entschlüsselt hat. Folgt die Substitution aber keinem bestimmten Muster, wie es Porta erwähnt oder wie es auch in den ursprünglichen Aufzeichnungen von Vigenère zu finden ist, erschwert dies eine mögliche Entschlüsselung. Interessant wäre daher zu wissen, welche Möglichkeit Leibniz bevorzugte; hätte er die Idee der beliebigen Substitution im Gegensatz zu Porta explizit dargestellt, wäre dies eine weitere kryptogaphiegeschichtliche Leistung gewesen. Bekannt ist, dass Leibniz beispielsweise seine eigene Labyrinthus-Chiffre verwendete bei der zuerst ein Codewort niedergeschrieben wird, man danach die verbleibenden Buchstaben des Buchstabs anhängt und damit am Ende Paare bildet, die die Grundlage für die Verschlüsselung bilden. Leibniz verwendete also keinen Shift, aber auch keine beliebige Anordnung.[28] Es wäre also von hier nur ein weiterer kleiner Schritt zu einer freien Alphabetanordnung und damit zu einem Zugewinn an kryptographischer Sicherheit; aufgrund mangelnder Quellenlage über Leibniz Gedankengänge kann diese interessante Frage aber leider nicht abschließend beantwortet werden.

Doch selbst, wenn die Alphabete nur in einem klassischen Shift-Verfahren angeordnet gewesen wären, hätte die Maschine zur damaligen Zeit nichtsdestotrotz ein extremes Maß an Sicherheit

[28] Badur 2016: 81

ermöglicht. Zwar ist die Grundidee des Suchens nach Bi- und Trigrammen schon bei Porta bekannt, doch wurde diese Art des Angriffs erst Mitte des 19. Jahrhunderts explizit formuliert, womit die Chiffriermaschine mit damaligen Mitteln nicht hätte gebrochen werden können. Selbst für den Fall, dass die von Kasiski und Babbage entwickelte Angriffsart mit den Bi- und Trigrammen schon damals bekannt gewesen wäre, hätte man die Leibniz-Maschine leicht nachrüsten können. So könnte man z.B. einfach größere Anzeigetrommeln mit mehr Alphabeten bzw. Staffelwalzen mit mehr Keilen und damit mehr Rotationsmustern verwenden. Auch könnte man, um die Sicherheit weiter zu erhöhen, nach einigen Wörtern die Einstellung der Staffelwalze bzw. das Alphabet auf der Anzeigetrommel ändern.[29] Die Maschine von Leibniz zeichnet sich durch ein modulares Design aus, was ein Nachrüsten in Bezug auf Sicherheit einfach bewerkstelligen lässt, ohne etwas an der kryptographischen Grundidee zu ändern.

Unter bestimmten Voraussetzungen war es aber bereits zu Leibnizens Lebzeiten möglich polyalphabetische Nachrichten zu entziffern, nämlich dann, wenn leicht zu erratende Schlüsselwörter oder Sprichwörter verwendet wurden. Ein Vorteil den die mechanisierte Art der Verschlüsselung der Machina Deciphratoria mit sich bringt liegt aber gerade darin, dass es kein kurzes Schlüsselwort gibt, dass sich periodisch wiederholt. Stattdessen merkt man sich die Ausgangstellung der Anzeigetrommel mi den verwendeten Alphabetleisten und der verwendeten Staffelwalze. Würde man dies in ein Schlüsselwort übersetzen, man erhielte lediglich eine willkürliche Buchstabenkombination, womit der Schlüssel nicht einfach erraten werden kann.[30] Ein unbefugtes Abfangen der Nachrichten wird also dadurch erschwert, dass ein Kryptoanalyst keine Informationen darüber hat, welcher Teil des Textes mit welcher Chiffre verschlüsselt ist, womit ein weiterer Vorteil der Leibniz-Maschine gegeben ist.[31] Allerdings ist auch die Machina Deciphratoria nicht unanfällig gegenüber menschlichen Fehlern. So kann theoretisch eine Verschlüsselung gebrochen werden, wenn bei mehreren Nachrichten der gleiche Schlüssel (Depths) verwendet wird oder periodisch auftauchende bzw. leicht zu erratende Satzbestandteile (Cribs bzw. Kisses) in den Chiffriertexten verwendet werden. In dieser Hinsicht ist auch die Machina Deciphratoria für die gleichen menschlichen Fehler anfällig, die z.B. auch zur Entschlüsselung der Enigma mit beigetragen haben.[32] Die Chiffriermaschine von Leibniz hätte also für damalige Verhältnisse ein extremes,

[29] Rescher 2012: 40
[30] Rescher 2012: 40
[31] Rescher 2012b: 6
[32] Ratcliff 2005: 282ff.

unübertroffenes Niveau an Sicherheit garantiert, allerdings sollte sie nicht grundsätzlich als unangreifbar angesehen werden.

Zusammengefasst weist die Maschina Deciphratoria damit folgende Eigenschaften auf: [33]

- Es gibt verschiedene Formen der Entschlüsselung
- Es ist eine Ver- und Entschlüsselung möglich
- Diese Maschine arbeitet in einfacherer Weise als die Rechenmaschine von Leibniz
- Die Ein- und Ausgaben müssen separat notiert werden; es gibt kein automatisches Notieren der verschlüsselten Nachricht, sondern man muss quasi per Hand mitschreiben
- Die Maschine ist klein und leicht zu transportieren

4.2. Geschichte der Machina Deciphratoria

Was die Geschichte der Geschichte der Chiffriermaschine von Leibniz betrifft, so ist hier vor allem das Jahr 1688 zu nennen. Im Oktober jenes Jahres bekam Leibniz eine langersehnte Audienz bei dem österreichischen Kaiser Leopold I. Die Monate davor verbrachte er mit ausführlichen Vorbereitungen und Notizen, um dem Kaiser seine verschiedenen Ideen und Vorstellungen angemessen präsentieren zu können und für deren Verwirklichung zu werben.[34] In diesen Notizen wird auch die vorgestellte Verschlüsselungsmaschine explizit erwähnt. So schreibt Leibniz im Original:

„Dergleichen sind meine Machina deciphratoria damit ein potentat mit vielen 10 ministris, in unterschiedenen 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 greiffen könne, also daß es gleich mit berührung der clavir darstehe, und nur abcopiret werden dürffe.“[35]

Weiterhin heißt es bei Leibniz:

„Aus gleichen principio wiewohl viel leichter, habe eine Machinam deciphratoriam vor hohe Personen ausgefunden. Ist eine kleine Machinula die leicht bey sich zu fuhren. Darauff kan ein großer herr viele fast unauflößliche Ciphern zugleich haben, und mit vielen Ministris correspondiren; weilen aber sowohl die stellung in Ziphern als das deciphriren mühsam, so bestehet die facilitat darinn, daß man die gegebene Ziphern oder buchstaben nur greiffen darff als wenn man auff einem clavicordio oder Instrument spielte, so kommen die begehrten augenblicklich herauß und stehen da; durffen denn nur abgeschrieben werden[.]“[36]

[33] Rescher 2011: 3
[34] Rescher 2012: 36
[35] A. IV 4: 27
[36] A. IV 4: 68

Was Leibniz hier also vorschlägt, ist eine automatische Maschine, die so einfach, wie ein Klavier bedient werden kann. Man muss also gewissermaßen nur spielen und ist nicht selber für eine konkrete Tonerzeugung verantwortlich, was den menschlichen Faktor eliminiert. Diese Hinweise in den Notizen zur kaiserlichen Audienz sind mit die deutlichsten für die Machina Deciphratoria in den Aufzeichnungen von Leibniz. Am Ende wünschte der österreichische Kaiser die Verwirklichung einiger Ideen und Pläne, die Chiffriermaschine war aber nicht darunter.[37] Wieso der Wiener Hof an einer solchen Maschine nicht interessiert war, darüber existieren keine belastbaren Quellen, weswegen hier nur gemutmaßt werden kann. Fakt ist, dass der Wiener Hof in der damaligen Zeit das beste Zentrum für Kryptoanalyse im europäischen Raum besaß. Die Österreicher wussten um ihren Ruf als Codebrecher und wussten auch, dass sie in Europa als konkurrenzlos galten; sie konnten also die Sicherheit ihrer eigenen Verschlüsselungstechniken im Vergleich zur europäischen Konkurrenz gut einschätzen und sie damit als ausreichend sicher einstufen. Ebenfalls könnte man die Konstruktion der Leibniz-Maschine als Schwäche auslegen: Wenn die Maschine leicht und transportabel ist, besteht damit das Risiko, dass sie eines Tages gestohlen wird und die Gegenseite so ein Verfahren erhält, die eigene Kommunikation abhörsicher zu gestalten. Ein Geheimhalten der Maschinenkonstruktion wäre nicht lange möglich gewesen, da es immer Sekretäre und anderer Personen bedurfte, um Nachrichten zu verschlüsseln bzw. zu entschlüsseln. Ab einem gewissen Umfang von Korrespondenz ist dies für einen einzelnen Diplomaten nicht mehr umsetzbar, weswegen andere Personen mit einbezogen werden müssen, was dann wiederum auch die Wahrscheinlichkeit erhöht, dass die Gegenseite von dem grundlegenden Prinzip der Verschlüsselung erfährt. Die Benutzung der Machina Deciphratoria hätte also womöglich zu einem kryptographischen Wettrüsten geführt, an dem man auch aus profitablen Gründen nicht interessiert war, da die Informationen aus der Schwarzen Kammer von Wien auch gerne an andere Staaten weiterverkauft wurden.[38] Eine andere und nüchterne Erklärung mag vielleicht ebenfalls sein, dass bei der Präsentation von Leibniz niemand aus der dortigen Schwarzen Kammer mit involviert war, der das Potential der Maschine adäquat einschätzen konnte.

Unter Umständen wäre die Chiffriermaschine aber womöglich auch anders realisiert worden. So wollte sich Leibniz im August 1716, im Zuge des Besuchs des englischen Königs George I. in Hannover bzw. Bad Pyrmont, u.a. mit dem jungen Philip Heinrich treffen.[39] Dieser Sohn seines Freundes Johann Ludwig Zollmann wurde in der Schwarzen Kammer von Hannover

[37] Rescher 2012: 37
[38] Singh 2000: 82
[39] Müller & Krönert 1969: 260

ausgebildet, bevor er nach England ging und dort zu einem der besten Kryptoanalysten des Landes aufstieg. Ein Treffen zwischen den beiden Personen war angesetzt, fand aber wegen Terminüberschneidungen am Ende doch nicht statt.[40] Hier ist zu spekulieren, ob Leibniz eine fachkundige Person von seiner Idee erzählt und diese das Potential seiner Erfindung erkannt hätte, die historischen Umstände aber eine solche Gelegenheit nicht zuließen.

Leibniz hatte zur damaligen Zeit 20.000 Gulden seiner eigenen Ersparnisse für die Konstruktion einer Rechenmaschine ausgegeben, dass entspricht in der heutigen Zeit einer Kaufkraft von ungefähr einer Million US-Dollar.[41] Die Kosten für die moderne Rekonstruktion der Machina Deciphratoria lagen bei mehr als 40.000 Dollar.[42] Dies ist signifikant weniger und damit zu erklären, dass die technische Realisierung einer solchen Chiffriermaschine viel einfacher möglich ist. So wird beispielsweise bei der Machina Deciphratoria nur eine Staffelwalze benötigt, bei der Rechenmaschine hingegen neun. Diese Anhaltspunkte lassen darauf schließen, dass Leibniz nicht unbedingt an der Realisierung einer solchen Chiffriermaschine interessiert war, obwohl er durchaus selber die finanziellen Möglichkeiten dazu gehabt hätte. Daher wird Leibniz diese Maschine nur als Möglichkeit angeboten haben, war aber nicht unbedingt an einer Verwirklichung von seiner Seite aus interessiert; dies besagt auch eine Notiz, in der Leibniz gegenüber den österreichischen Offiziellen betont, dass er konkrete Details einer solchen Maschine niemanden gegenüber erwähnt hat.[43] Der Einsatz war damit klar für den politischen Bereich bestimmt.

Aufschluss auf die Motivation von Leibniz gibt auch die Passage eines seiner Briefe an den Herzog Ernst August von Hannover aus den Jahren 1685-87:

„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.“[44]

Leibniz war damit an ganzen Produktsystemen interessiert, die gemeinsame wichtige Bauteile enthalten. Dementsprechend muss seine Chiffriermaschine in Verbindung mit seiner Rechenmaschine gesehen werden.[45] Leibniz wollte die Welt hauptsächlich verstehen, nicht unbedingt gestalten, weswegen er die Realisierung seiner Chiffriermaschine nicht weiter verfolgte; im Gegensatz zu der Machina Arithmetica, die er bis zu seinem Tod versuchte

[40] Rescher 2011: 9
[41] Rescher 2011: 9
[42] HAZ 2015
[43] A. IV 4: 27
[44] Stein 2014: 3 (Aus dem Französischen)
[45] Stein 2014: 3

fertigzustellen. Unter diesen Umständen ist sein berühmter Ausspruch „Calculemus!“, also „Lasst uns rechnen!“ zu nennen; es geht darum die Welt mit mathematischen und logischen Methoden zu verstehen.

Vom technischen Stand hätte seine Maschine das fortschrittlichste Chiffrierverfahren ihrer Zeit garantiert und hätte die polyalphabetische Verschlüsselung bezüglich ihrer Schnelligkeit und Sicherheit auf ein völlig neues Niveau gehoben. Selbst viele Jahrzehnte später wurde bei Fragen der Verschlüsselung mit weniger Aufwand bzw. Mitteln vorgegangen. So gab es z.B. im Amerikanischen Bürgerkrieg von 1861-1865 auf Seiten der Südstaaten gar keine kryptologische Stelle. Hier wurde vorrangig mit Codebüchern hantiert, deren Basis zu dieser Zeit beispielsweise weit verbreitete Englisch-Wörterbücher darstellten. Erst später im Verlauf des Krieges wurde auf die Vigenère-Verschlüsselung umgestiegen. Aber auch dann enthielten die Botschaften der Südstaaten oftmals Chiffrierfehler, die damit einen Rückschluss auf den verwendeten Schlüssel ermöglichten. Die Nordstaaten auf der anderen Seite waren professioneller organisiert, allerdings beschäftigten sich auch in ihrer Armee lediglich drei Personen mit der Entzifferung von Nachrichten.[46]

Damit gesehen ist die Leibniz-Maschine eine technische Errungenschaft, die weit vor ihrer Zeit entstanden ist und deren kryptographische Sicherheit erst gegen Ende des I. Weltkriegs wieder erreicht wurde. Abbildung 5 verdeutlicht, dass das Zeitalter der mechanischen Verschlüsselungsmaschinen erst mit dem I. Weltkrieg begann; die Machina Deciphratoria, die diese Idee vorwegnahm, erscheint daher als einmalige historische Anomalie und markiert damit frühzeitig den Übergang von Kryptographiegeräten hin zu Kryptographiemaschinen.[47] Man kann die Leibniz-Maschine damit als eine Art Proto-Enigma ansehen und das gute 200 Jahre vor der hauptsächlichen Nutzung von Rotor-Chiffriermaschinen.[48]

Das Potential der Leibniz-Maschine wurde aber zur damaligen Zeit nicht erkannt, was auch an einigen unglücklichen Zufällen und Begebenheiten gelegen haben mag. Dieses Nicht-Weiterverfolgen bzw. nicht zur Kenntnis nehmen trifft aber auch für andere Entwicklungen in der Geschichte der Kryptographie zu. So entwickelte beispielsweise Charles Babbage in den 1840er Jahre eine Lösung für die Vigenère-Verschlüsselung, die er jedoch nicht publizierte. Deswegen wird diese Leistung oftmals allein dem preußischen Offizier Friedrich Kasiski zugeschreiben, der die Verschlüsselung erst einige Jahre nach Babbage eigenständig brechen

[46] Schmeh 2008: 21
[47] Rescher 2012: 42
[48] Rescher 2011: 7

konnte. Eine ähnliche Situation gab es auch in den 1970er Jahren, wo die grundlegende Idee der asymmetrischen Verschlüsselung bereits von James Ellis, Clifford Cocks und Malcom Willliamson bei ihrer Arbeit für den britischen Geheimdienst GCHQ entdeckt wurde, es aber aus Gründen der Geheimhaltung zu keiner Publikation kam. Den öffentlichen Ruhm und die Anerkennung erhielten wenige Jahre später dann Ronald Rivest, Adi Shamir und Leonard Adleman.[49]

Display A

The Four Historical Stages of Cryptanalysis

I. Pen and Pencil Amateurism (up to ca. 1690)

↓ War of the Spanish Succession (1690-1710)

II. Complexity Management by Mathematical Sophistication (ca. 1690-ca. 1915)

↓ WWI (1914-1918)

III. Mechanical Contrivances [compound gears, telephone rotors] (ca. 1915-ca. 1940)

↓ WW II (1939-1945)

IV. Electronic Calculators (after ca. 1943)

(Abbildung 5)[50]

[49] Singh 2000: 338ff.
[50] Rescher 2012: 40

5. Quellenverzeichnis

Primärliteratur

A. - Leibniz Gesammelte Werke, es wurde gemäß der Ausgabe der Deutschen Akademie der Wissenschaften in folgender Reihenfolge zitiert: Serie, Jahrgang, Seite(n)

Sekundärliteratur

Badur, Klaus. 2016. *Die Vorfahren der Enigma und des Computers.* Spektrum der Wissenschaft September 2016: 76–87.

Kahn, David. 1996. *The Codebreakers.* The Story of Secret Writing. New York, NY: Scribner.

Müller, Kurt und Gisela Krönert 1969. *Leben und Werk von G. W. Leibniz: Eine Chronik* Frankfurt am Main: Vittorio Klosterman.

Ratcliff, R. A. 2005. How Statistics Led the German to Believe Enigma Secure and Why They Were Wrong: Neglecting the Practical Mathematics of Cipher Machines. In *The German Enigma Cipher Machine*, Hrsg. Brian J. Winkel, Cipher Deavors, David Kahn, Louis Kruth, 275-287. Boston: Artech House.

Rescher, Nicholas. 2012. Leibniz and Cryptography. An Account on the Occasion of the Initial Exhibiton of the Reconstruction of Leibniz's Cipher Machine. Pittsburgh: University Library System, University of Pittsburgh.

Schmeh, Klaus. 2008. *Codeknacker gegen Codemacher.* Die faszinierende Geschichte der Verschlüsselung. Herdecke/Dortmund: W3L-Verlag.

Singh, Simon. 2000. *Geheime Botschaften.* Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet. München/Wien: Hanser.

Symonds, John Addington. 1927. *Renaissance in Italy: Italien Literature.* London: John Murray.

Internetdokumente *(Zugriff letztmals am 26.06.2017)*

Hannoversche Allgemeine (HAZ) 2015: *Geheimcode Leibniz*

http://www.haz.de/Hannover/Aus-der-Stadt/Uebersicht/Tueftler-bauen-Chiffrierapparat-von-Gottfried-Wilhelm-Leibniz-nach

Rescher, Nicholas. 2011. *Leibniz's Machina Deciphratoria.*

http://philsci-archive.pitt.edu/8499/1/Leibniz's_Machina_English_Version.docx

Stein, Erwin. 17.11.2014. *Eine „Machina Deciphratoria" nach Gottfried Wilhelm Leibniz*. Pressemitteilung

https://www.uni-hannover.de/fileadmin/luh/content/webredaktion/universitaet/geschichte/leibniz/Presseinformation_Machina_Deciphratoria.pdf

Wikipedia 2010: *Staffelwalze* (erstellt von User Ezrdr)

https://de.wikipedia.org/wiki/Staffelwalze#/media/File:Cylindre_de_Leibniz_anim%C3%A9.gif

Bonus

Die Machina Deciphratoria ‚live' in Betrieb:

https://www.youtube.com/watch?v=puYnYrDdgvw&t=173s