D I P L O M A R B E I T

Kryptologie und deren Einbau im Mathematikunterricht

ausgeführt am
Institut für Diskrete Mathematik und Geometrie
der Technischen Universität Wien
Wiedner Hauptstraße 8-10
1040 Wien

unter der Anleitung von
Ao. Univ.-Prof. Mag. Dr. Manfred Kronfellner

durch
Mathias Buzek
Schliefbergstraße 3/2
2100 Leobendorf

Wien am 27.04.2012

0 Vorwort

Das Thema Verschlüsselung fasziniert mich, seitdem ich in meiner eigenen Schulzeit das erste Mal damit konfrontiert wurde. Aus diesem Grund erschien mir diese Thematik für meine Diplomarbeit als ideale Wahl. Doch sollte bei der Arbeit auf jeden Fall ein Ergebnis entstehen, aus dem ich für meine spätere Lehrtätigkeit einen Nutzen ziehen kann. Aus diesem Grund kam die Idee auf, die Arbeit so aufzubereiten, dass dieses, mich fesselndes, Thema im Schulunterricht umgesetzt werden kann.

Dankenswerterweise erklärte sich Herr Mag. Dr. Manfred Kronfellner bereit, mich bei dieser Arbeit zu betreuen und unterstützte mich während dieser Zeit mit wertvollen Hinweisen und Informationen.

Bedanken möchte ich mich auch bei meiner Familie, die mich während meiner Studienzeit immer unterstützt hat. Besonders möchte ich meiner Mutter danken, ohne deren Einfluss ich mich vermutlich nicht für das Studium entschieden hätte und jetzt nicht an dieser Stelle wäre.

Weiters möchte ich ein besonderes Dankeschön an meine Freundin richten, die mich während meines Studiums, speziell aber in den letzten, anstrengenden Monaten, immer großartig unterstützt hat.

Wien am 27.04.2012 MATHIAS BUZEK

1 Inhaltsverzeichnis

2 Einleitung

Diese Arbeit thematisiert die Kryptologie und zeigt Umsetzungsmöglichkeiten für den Schulunterricht auf. Das Ziel dieser Arbeit ist, Anregungen für den Mathematikunterricht zu geben. Dabei wird die Thematik so eingegrenzt, dass sie für den Schulunterricht umsetzbar ist. Es werden jedoch keine fertigen Unterrichtsplanungen erstellt.

Zu Beginn werden einige begriffliche und kryptographische Grundlagen erläutert und definiert, da auf diese im Umgang mit dem Thema nicht verzichtet werden kann. Auch bei der Bearbeitung der Thematik im Schulunterricht sollten von Beginn an die korrekten fachlichen Begriffe verwendet werden.

Im zweiten Teil wird die geschichtliche Entwicklung der Kryptologie thematisiert. Dabei wird ausschließlich auf den geschichtlichen Inhalt eingegangen. Es werden in diesem Abschnitt keine Beispiele behandelt und auch keine detaillierten Funktionsweisen von kryptographischen Verfahren bearbeitet.

Im Anschluss erfolgen Erläuterungen zu einigen herausgegriffenen klassischen Verschlüsselungsverfahren und in weiterer Folge auch zu einigen modernen Verfahren. Diese beiden Teile sind so aufgebaut, dass sie einerseits zur Information für eine Lehrperson dienen, andererseits befinden sich auch Vorschläge für Aufbaumöglichkeiten und Beispiele für den direkten Einsatz im Schulunterricht darin.

Eine nähere Ausführung der Funktionsweisen von den Verschlüsselungsmaschinen erfolgt nicht, da die Behandlung dieser Thematik für den Schulunterricht eher von geringerer Bedeutung ist und den Rahmen dieser Arbeit übersteigen würde. Natürlich kann die Funktionsweise der einen oder anderen Maschine erläutert und besprochen werden. Hierzu könnte der bekannteste Vertreter – die Enigma – herangezogen werden. Es wird im Unterricht jedoch nicht die

Zeit sein, um näher darauf einzugehen. Außerdem hält sich der mathematische Gehalt dieser Maschinen in Grenzen.

Im letzten Teil wird der Bezug zum Schulunterricht in den einzelnen Abschnitten dargestellt. Hierbei wird einerseits die Rechtfertigung für eine Behandlung der Thematik gegeben. Andererseits wird auch für die einzelnen Verfahren angegeben, auf welche Lehrinhalte des Lehrplans Bezug genommen werden kann und in welcher Schulstufe die Inhalte behandelt werden können.

Abgerundet wird die Arbeit durch die Angabe einiger angehängter Beispiele, Aufgabenstellungen und Demonstrationsmöglichkeiten, wie sie bei den einzelnen Themen im Unterricht eingebaut und gestellt werden können.

3 Grundlagen

3.1 Einleitung

Seit Jahrtausenden versuchen Menschen Nachrichten zu übermitteln. Dabei ist ein großes Ziel bei manchen Nachrichten, dass sie nur von denjenigen gelesen werden, für die sie auch gedacht sind. Um dieses Ziel zu erreichen gibt es mehrere Möglichkeiten. Eine Möglichkeit ist, die Nachricht zu verbergen, sodass dessen Existenz nicht jeder Person bekannt ist. Diese Vorgehensweise wird in der Wissenschaft als Steganographie bezeichnet. Dieses Wort setzt sich aus den beiden altgriechischen Teilen „steganos“ für „bedeckt“ und „graphein“ für „schreiben“ zusammen. Eine weitere Möglichkeit ist, die Nachricht nicht zu verbergen, sondern zu verschlüsseln, sodass sie unlesbar ist. Sie ist dann nur durch eine bestimmte Entschlüsselungsvorschrift, meist unter Zuhilfenahme eines bestimmten Codeworts, zu entziffern. Diese Vorgehensweise wird in der Wissenschaft als Kryptographie bezeichnet.[1]

Dabei ist das Ziel der Kryptographie einige Grundprobleme zu lösen. Zu diesen zählen neben der bereits erwähnten Geheimhaltung, also dem unlesbar Machen einer Nachricht für Unbefugte, auch Integrität, Authentifikation und Verbindlichkeit. Unter Integrität wird verstanden, dass eine abgeschickte Nachricht auf dem Übertragungsweg nicht unbefugt verändert werden kann. Unter Authentifikation wird der Identitätsnachweis eines Absenders verstanden, also die Sicherstellung, dass sich niemand als eine andere Person ausgeben kann. Unter Verbindlichkeit wird etwas Ähnliches verstanden. Es handelt sich dabei ebenfalls um die eindeutige Zuordenbarkeit einer Nachricht zur Senderin bzw. zum Sender, allerdings mit dem zusätzlichen Augenmerk darauf, dass ein späteres Abstreiten des Versandes einer Nachricht nicht möglich ist. Es soll also belegt sein, dass die Nachricht von einer bestimmten Person geschickt wurde.[2]

[1] vgl. ECKERT 2004, S. 281
[2] vgl. BEUTELSPACHER u.a. 2010, S. 1 ff; ERTEL 2007, S. 19

Sicherheit

Eine weitere wichtige Eigenschaft kryptographischer Verfahren ist die Sicherheit desselbigen. Hierzu muss zunächst geklärt werden, was unter Sicherheit verstanden wird. Dabei wird zwischen absoluter und praktischer Sicherheit unterschieden. Absolute Sicherheit wird dann erreicht, wenn durch Abfangen des Geheimtextes absolut keine Information gewonnen werden kann. Dies ist jedoch nur dann der Fall, wenn es genauso viele Schlüssel wie Klartexte gibt. Anders ausgedrückt bedeutet dies, dass der Schlüssel gleich lang sein soll, wie der zu verschlüsselnde Text. Dies erfüllt nur ein einziges Verschlüsselungssystem – das One-Time-Pad, auf das in Kapitel 6.6 noch eingegangen wird. Bei Verschlüsselungsverfahren, die heutzutage eingesetzt werden, wird nicht absolute Sicherheit sondern praktische Sicherheit gefordert. Dies bedeutet, dass der Aufwand eine Nachricht zu entschlüsseln, dessen Wert übersteigt.[3]

3.2 Begriffsbestimmungen

So wie alle Wissenschaften, besitzt auch die Kryptologie eine eigene Fachsprache. Die wichtigsten Vokabeln müssen zunächst kurz definiert werden, bevor mit ihnen gearbeitet werden kann.

Das Wort Kryptographie setzt sich aus den beiden griechischen Worten „kryptos“ für „verborgen“ und „graphein“ für „schreiben“ zusammen. ERTEL[4] versteht unter dem Begriff „die Lehre der Absicherung von Nachrichten durch Verschlüsseln“. KÜSTERS und WILKE[5] fassen den Begriff allgemeiner auf und bezeichnen Kryptographie als „Chiffrieren (das Verschlüsseln)“. Eine sehr ausführliche Definition ist in ECKERT[6] zu finden. Dort heißt es „unter der Kryptographie versteht man die Lehre von den Methoden zur Ver- und Entschlüsselung von Nachrichten zum Zweck der Geheimhaltung von Informationen gegenüber Dritten (Angreifern)“.

[3] vgl. JANOWICZ 2006, S. 10 ff; KLEIN 2007, S. 21 f
[4] ERTEL 2007, S. 18
[5] KÜSTERS & WILKE 2011, S. 3
[6] ECKERT 2004, S. 281

Als Kryptoanalyse wird die gegengesetzte Wissenschaft bezeichnet. ERTEL[7] bezeichnet sie als „Kunst, Chiffretext[e] aufzubrechen“ während ECKERT[8] sie als „Wissenschaft von den Methoden zur Entschlüsselung von Nachrichten, ohne Zugriff auf den verwendeten Schlüssel zu haben“, bezeichnet. Kryptographie und Kryptoanalyse bilden zusammen die Kryptologie.

Ein kryptographischer Algorithmus bezeichnet eine mathematische Funktion, die beim Verschlüsseln den Klartext *M* (Message) in einen Geheimtext *C* (Cypher) überführt und beim Entschlüsseln den umgekehrten Weg bildet. Hierzu wird ein Schlüssel *K* (Key) benötigt. Die Verschlüsselungsfunktion wird im Folgenden mit *E* (Encrypt) bezeichnet, die Entschlüsselungsfunktion mit *D* (Decrypt). Im symmetrischen Fall sind die verwendeten Schlüssel bei der Verschlüsselung und der Entschlüsselung identisch. Im asymmetrischen Fall werden unterschiedliche Schlüssel genutzt. Für asymmetrische Verfahren gilt der Zusammenhang:

$$E_{K1}(M) = C$$
$$D_{K2}(C) = M$$
$$D_{K2}(E_{K1}(M)) = M$$

Die Zusammenhänge bei symmetrischen Verfahren sind dieselben, wobei in diesem Fall *K1 = K2* gilt.[9]

Kerckhoffs Prinzip

Eine wichtige Anforderung, die an heutige kryptographische Verfahren gestellt wird, ist das Kerckhoffsche Prinzip[10]. Diese These besagt, dass die Sicherheit eines Verschlüsselungsverfahrens einzig und allein im Schlüssel liegen darf. Anders formuliert bedeutet dies, dass selbst wenn möglichen Angreiferinnen und Angreifern die Funktionsweise eines Verfahrens und der chiffrierte Text zur

[7] ERTEL 2007, S. 18
[8] ECKERT 2004, S. 281
[9] vgl. ERTEL 2007, S. 19
[10] Benannt ist dieser Grundsatz der modernen Kryptologie nach dem niederländischen Linguisten und Kryptologen Auguste Kerckhoffs (1835 - 1903), der ihn 1883 formulierte.

Verfügung stehen, diese keine Rückschlüsse auf den Klartext ziehen können. Anders ausgedrückt, soll in obiger Notation selbst bei Kenntnis der Ver- und Entschlüsselungsfunktionen *E* und *D* nicht von der verschlüsselten Nachricht *C* auf den Klartext *M* geschlossen werden können, wenn die beiden Schlüssel *K1* und *K2* unbekannt sind. Die geschichtlichen Ereignisse und Erfahrungen verdeutlichen die Wichtigkeit dieses Prinzips, was in Kapitel 4 (Geschichtliche Entwicklung der Kryptographie) noch behandelt wird.[11]

Angriffsszenarien

Dies bedeutet jedoch auch, dass ein Verfahren nur dann als sicher gelten kann, wenn es einer Reihe von möglichen kryptoanalytischen Angriffen auf jeden Fall widersteht. Zu diesen Angriffen zählen neben Brute-Force-Angriffen, bei denen mögliche Schlüssel durch bloßes Probieren getestet werden, auch vier weitere Angriffsszenarien.

Zu diesen zählt einerseits der Cyphertext-Only-Angriff, bei dem die Angreiferin bzw. der Angreifer lediglich den Geheimtexten kennt und mit diesem versucht den Klartext zu ermitteln. Dieses Angriffsszenario ist das wahrscheinlichste, da die verschlüsselte Nachricht meist relativ einfach abgefangen werden kann. Zugleich handelt es sich dabei allerdings auch um den schwächsten möglichen Angriff, da die meisten Verfahren diesbezüglich gerüstet sind.

Ein zweites Angriffsszenario bildet der Known-Plaintext-Angriff, bei dem die Angreiferin bzw. der Angreifer zusätzlich zum verschlüsselten Geheimtext auch noch den zugehörigen Klartext kennt. Dies könnte beispielsweise bei der Übermittlung eines Briefs der Fall sein. Briefe starten und enden üblicherweise stets mit denselben Floskeln, welche für einen solchen Angriff genutzt werden könnten. Mithilfe der beiden Texte wird versucht den Schlüssel zu ermitteln, mit welchem anschließend auch weitere verschlüsselte Nachrichten entschlüsselt werden könnten.

[11] vgl. SCHMEH 2004, S. 13 f

Ein weiteres Szenario bildet der Chosen-Plaintext-Angriff. Hier kann die Angreiferin bzw. der Angreifer den Klartext beliebig vorgeben und dadurch den zugehörigen Geheimtext ermitteln. Dies ist beispielsweise bei jedem asymmetrischen Verfahren möglich, da ja der Schlüssel für die Verschlüsselung einer Nachricht öffentlich zugänglich ist. Daher zählt auch diese Angriffsvariante zu den häufigsten.

Das letzte Angriffsszenario bildet der Chosen-Cyphertext-Angriff, bei dem die Angreiferin bzw. der Angreifer durch Vorgabe eines kodierten Textes den dazugehörigen Klartext bestimmen kann. Dieses Angriffsszenario ist das unwahrscheinlichste der vier genannten.[12]

Hält ein Verschlüsselungsverfahren all diesen Angriffen stand, so kann es als sicher bezeichnet werden. Standhalten kann dabei bedeuten, dass der Aufwand zum Erlangen der Daten dessen Wert übersteigt oder die benötigte Zeit zum Erlangen der Daten größer ist als die Zeit, die die Daten geheim sind.[13]

Primzahlen in der Kryptologie

Eine wichtige Rolle bei heutigen Verfahren spielen die Primzahlen. Aus diesem Grund ist es notwendig, sich auch mit diesem mathematischen Phänomen zu beschäftigen. Unter einer Primzahl wird „eine natürliche Zahl $p \neq 1$ [verstanden], die nur durch p und 1 teilbar ist.“[14] Offensichtlich muss bei dieser Definition noch die *0* ausgeschlossen werden, da diese zwar zu den natürlichen Zahlen zählt, allerdings auch keine Primzahl ist. Bei heutigen Verfahren werden große Primzahlen benötigt, weshalb sich zunächst die Frage stellt, ob es unendlich viele Primzahlen gibt. Bereits die alten Griechen wussten, dass dem so ist. Es bleibt also noch die Frage, ob auch beliebig große Primzahlen gefunden werden können. Deshalb wird in einem ersten Schritt überlegt, wie Primzahlen statistisch verteilt sind. Werden die ersten auftretenden Primzahlen betrachtet, so

[12] vgl. STOHR 2007, S. 25
[13] vgl. PAAR & PELZL 2010, S. 9 ff; ERTEL 2007, S. 24 f
[14] BEUTELSPACHER u.a. 2010, S. 119

kann vermutet werden, dass je größer die betrachteten Zahlen sind, umso weniger Primzahlen in einem Bereich auftreten. Die Primzahldichte sinkt also:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, …

Im Intervall [1,15] treten sechs Primzahlen auf, währen im Bereich [46, 60] nur noch drei Primzahlen auftreten. Allerdings kann auf den ersten Blick keine Regelmäßigkeit im Vorkommen von Primzahlen erkannt werden. Tatsächlich folgen diese keiner bislang bekannten Gesetzmäßigkeit. Dennoch kann die Wahrscheinlichkeit angegeben werden, dass eine zufällig gewählte natürliche Zahl eine Primzahl ist. Diese folgt aus dem Primzahlsatz und kann durch

$$P(p \text{ ist prim}) = \frac{2}{ln(p)}$$

ermittelt werden. Die genaue Herleitung dieser Berechnung soll hier nicht behandelt werden, kann jedoch beispielsweise bei PAAR & PELZL[15] nachgeschlagen werden. Aus diesem Zusammenhang ergibt sich, dass für die Findung einer Primzahl mit einer Länge die bei heutigen Verschlüsselungsverfahren notwendig ist – das sind Zahlen mit etwa 154 dezimalen Stellen – die Überprüfung von durchschnittlich 177 zufälligen Zahlen notwendig ist. Nachgerechnet werden kann dies, indem in obiger Formel für $p = 10^{154}$ eingesetzt wird.[16]

Wie solche Primzahlen nun wirklich gefunden werden können wird in Kapitel 6.7 (Primzahltests) behandelt.

[15] vgl. PAAR & PELZL 2010, S. 187 f
[16] vgl. MATTHES 2003, S. 174 ff; PAAR & PELZL 2010, S. 187 f

4 Geschichtliche Entwicklung der Kryptographie

4.1 Einleitung

Dieses Kapitel gibt einen Überblick über die geschichtliche Entwicklung der Verschlüsselungsverfahren. Dabei werden drei Epochen unterschieden: die klassische Kryptographie, also die ersten Verschlüsselungsverfahren, welche von Hand durchgeführt wurden, das Zeitalter der Verschlüsselungsmaschinen und die moderne Kryptographie, welche mittels Computereinsatz arbeitet. Dabei liegen die Anfänge der Verschlüsselung bereits 3.500 Jahre zurück. Aus dieser Zeit stammt das älteste kulturhistorische Dokument, das die Existenz von Kryptologie belegt - eine mesopotamische Tontafel, auf der veränderte, und dadurch unlesbar gemachte, Keilschriftzeichen zu finden sind.[17]

Die Methoden der heutigen Kryptographie haben sich im Vergleich zu damals stark geändert. Das Ziel ist jedoch immer noch dasselbe. Die Entwicklung der Verschlüsselungsverfahren wurde seit der mesopotamischen Tontafel stets vorangetrieben. Verschlüsselungen wurden dechiffriert, was die Verfahren nutzlos machte. Dies wiederum hatte zur Folge, dass neue, verbesserte Verfahren entwickelt werden mussten. Das Wechselspiel zwischen Kryptographen – dem Verschlüsselnden – und Kryptoanalytiker – dem Entschlüsselnden – erreichte in den letzten 40 Jahren einen bis heute anhaltenden Höhepunkt. Begründet ist dies dadurch, dass die Kryptologie um 1970 zu einer akademischen Disziplin wurde, welche an Universitäten gelehrt und betrieben wird.[18]

4.2 Verschlüsselung von Hand

Wie bereits erwähnt, gehen die ersten belegten Verschlüsselungen 3.500 Jahre in die Vergangenheit zurück. Wie sämtliche anderen Entwicklungsgeschichten, machte auch die Kryptologie in den ersten Jahrhunderten nur sehr langsame

[17] vgl. WRIXON 2006, S. 238 ff, S. 281 ff
[18] vgl. SCHMEH 2004, S. 2

Fortschritte. Das Zeitalter der händischen Verschlüsselung begann etwa 1.500 v. Chr. und endete um 1920. Die ersten kryptographischen Verfahren waren geprägt von Transposition und Substitution. Bei der Transposition handelt es sich um eine neue Anordnung der Buchstaben, während unter Substitution ein Ersetzen der Buchstaben verstanden wird.[19]

Monoalphabetische Verschlüsselung durch Substitution

Bei der zuvor erwähnten mesopotamischen Tontafel handelt es sich um einen Vertreter der Substitutionsverschlüsselung. Die Buchstabensymbole werden so verändert, dass neue Symbole entstehen. Ein weiteres bekanntes Beispiel ist der monoalphabetische Cäsar-Code, bei dem die Buchstaben durch einen anderen ersetzt werden, welcher um eine frei wählbare aber feste Anzahl an Stellen im Alphabet verschoben steht. Dabei wird bei der Stellenanzahl um die verschoben wird, vom Schlüssel gesprochen.[20]

Die beiden Verfahren sind jedoch recht primitiv. Durch eine Häufigkeits- oder Frequenzanalyse kann sehr einfach festgestellt werden, um wie viele Stellen das Alphabet verschoben wurde bzw. welches geheime Symbol welchem Klartextsymbol entspricht. Das Verfahren der Transposition hat ihren Ursprung bei den alten Griechen. Bei der sogenannten Skytale, einem Instrument, das zur Verschlüsselung eingesetzt wurde, schrieben die Griechen die Nachricht auf einen Pergamentstreifen, der zuvor um einen runden Stab gewickelt wurde. Nach Entfernung des Streifens, war die Nachricht erst wieder zu lesen, wenn der Pergamentstreifen erneut um einen Stab mit gleichem Durchmesser gerollt wurde. Doch auch diese Permutationschiffren, bei denen lediglich die Reihenfolge der Zeichen verändert werden und diese somit an einem anderen Platz stehen, die Zeichen also permutiert werden, sind nicht sehr sicher. Da die Zeichen nicht verändert wurden, kann durch bloßes Ausprobieren der Klartext zurückgewonnen werden.[21]

[19] vgl. LUNDE 2009, S. 66 ff
[20] vgl. SCHMEH 2004,S. 6 ff; KIPPENHAHN 2006, S. 80 ff
[21] vgl. WRIXON 2006, S. 134 ff

Polyalphabetische Verschlüsselung

Der nächste große Entwicklungsschritt geschah erst, als der italienische Architekt, Mathematiker, Komponist und Philosoph Leon Alberti um 1460 eine Chiffrierscheibe entwickelte, welche im Grunde wie das Cäsar-Verfahren funktioniert. Er wechselte jedoch stets zwischen zwei verschiedenen Einstellungen, sodass eine Häufigkeitsanalyse erschwert wurde und setzte damit einen entscheidenden Schritt in Richtung der polyalphabetischen Verschlüsselung. Das Verfahren wurde über Jahre weiterentwickelt bis es der Franzose Blaise de Vigenère[22] im 16. Jahrhundert perfektionierte. Die Vigenère-Verschlüsselung verbindet den Klartext mit einem sich wiederholenden Verschlüsselungswort zu der codierten Nachricht. Diese Methode galt 300 Jahre lang als absolut sicher und wurde aus diesem Grund auch *Chiffre indèchiffrable* genannt.[23]

Entschlüsselung des Chiffre indèchiffrable

Doch 1863 veröffentlichte Friedrich Kasiski[24] eine Methode, mit der auch dieser scheinbar nicht zu entschlüsselnde Code geknackt werden kann. Durch die Beobachtung, dass in einem Text bestimmte Buchstabenkombinationen öfters auftreten als andere, kann auf die Schlüssellänge rückgeschlossen werden. Ist diese bekannt, kann der verschlüsselte Text in Teilblöcke gegliedert werden. Jeder dieser einzelnen Teilblöcke kann nun wiederum, analog zur monoalphabetischen Verschlüsselung, mit Hilfe der Häufigkeitsanalyse entschlüsselt werden.[25]

Neben diesem Kasiski-Test wurde das Ende der Verschlüsselungen von Hand zu dieser Zeit durch die zunehmend schnellere Nachrichtenübertragung eingeläutet. Durch die moderneren Kommunikationswege stieg die Chance, Nachrichten abzufangen. In den folgenden Jahren wurden viele Kriege, darunter der

[22] Blaise de Vigenère (1523 - 1596) war ein französischer Diplomat und Kryptograph, der nach seinem Dienst als Diplomat über 20 Bücher schrieb, die sich mit Kryptographie beschäftigten. Darunter befand sich auch die nach ihm benannte Vigenère-Verschlüsselung.
[23] vgl. SCHMEH 2004, S. 9 ff; LUNDE 2009, S. 72 f
[24] Der preußische Infanteriemajor Friedrich Wilhelm Kasiski (1805 - 1881) veröffentlichte in seinem Buch „Die Geheimschriften und die Dechiffrierkunst“ sein Verfahren, das bis heute noch unter seinem Namen bekannt ist.
[25] vgl. ERTEL 2007, S. 38 ff; MATTHES 2003, S. 110 f

amerikanische Bürgerkrieg und der erste Weltkrieg, unter anderem dadurch wesentlich beeinflusst, welche Seite die bessere Kryptoanalyse aufzubieten hatte.[26]

4.3 Verschlüsselungsmaschinen

Nach den großen Erfolgen der Codeknackerinnen und Codeknacker im ersten Weltkrieg mussten die Entwicklerinnen und Entwickler der Verschlüsselungsverfahren nachziehen. Die neuen Verschlüsselungsmethoden arbeiteten nun nicht mehr mit Papier und Bleistift. Es wurden komplexe Maschinen entwickelt, welche mit Hilfe elektrischer Signale Buchstaben in unterschiedlichster Weise vermischen und aufeinander abbilden konnten. Dabei wurden zur gleichen Zeit von mehreren Konstrukteuren weitgehend unabhängig solche Maschinen konstruiert. Einige werden im Folgenden etwas genauer behandelt.[27]

Die ersten Maschinen

Eine der ersten Verschlüsselungsmaschinen war die Kryha-Chiffriermaschine, die 1923 auf den Markt gebracht wurde. Auch wenn dies auf den ersten Blick so aussieht, leitet sich der Name nicht vom griechischen Wort „kryptos“ ab. Die Maschine ist nach dem gleichnamigen deutschen Entwickler benannt. Es handelte sich dabei um eine Chiffrierscheibe, die eine Substitutionsmethode realisiert. Das Besondere an dieser ist jedoch, dass sie per Knopfdruck eine neue Stellung einnimmt. Grundidee war, dass der Knopf beim Verschlüsseln nach jedem Buchstaben betätigt wird, und so ein zufällig erscheinender Schlüssel gebildet wird. Durch geschickte Vermarktung wurde aus der Maschine ein Verkaufsschlager. Sie verbreitete sich bis in die USA, wo William Friedman[28] mit

[26] vgl. SCHMEH 2004, S. 15 ff
[27] ebd, S. 43
[28] Der in Russland geborene William Frederick Friedman (1891 - 1969) war ein angesehener US-amerikanischer Kryptologe, der im zweiten Weltkrieg eine wichtige Rolle in den Entschlüsselungen durch das amerikanische Militär spielte. Im Gegensatz zu vielen anderen Kryptologen schrieb Friedman kaum Werke, sondern erzielte lediglich praktische Ergebnisse. Neben seinem Verfahren zur Entschlüsselung der Vigenère-Chiffre, knackte sein Team einerseits diverse japanische Verschlüsselungsmaschinen vor und während des zweiten Weltkriegs und entwickelte andererseits die SIGABA, die zur einzigen nicht geknackten Maschine wurde.

der Entschlüsselung der Maschine aufdeckte, dass sie wesentlich weniger Sicherheit bot als angenommen.[29]

In Amerika entstand im selben Zeitraum die erste Rotormaschine. Dieser liegt eine ähnliche Grundidee wie der Kryha-Maschine zugrunde. Dabei wird über eine Schreibmaschinentastatur eine kreisrunde Scheibe angesteuert, die den Buchstaben zu einem anderen verschlüsselt. Dies funktioniert über 26 eingehende Kontakte, die mit jeweils einem ausgehenden Kontakt verbunden sind. Durch Betätigen einer Taste wird nun über die Verschlüsselungsscheibe eine entsprechende Lampe zum Leuchten gebracht. Diese wiederum steht für den Geheimbuchstaben. Die folgende Abbildung zeigt die Funktionsweise in vereinfachter Weise für vier Buchstaben:

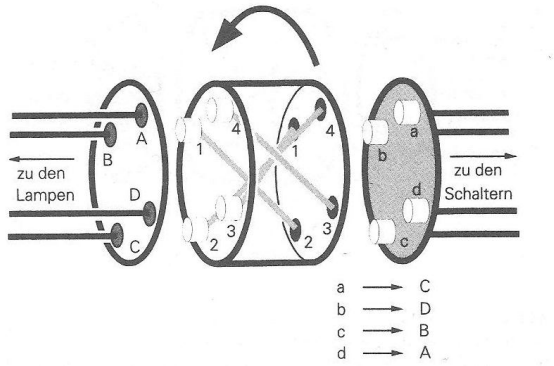

Abbildung 1: Die Kreisscheibe der Rotormaschine[30]

Wie schon bei der Kryha-Maschine, wird auch bei Rotormaschinen nach jedem Druck die Scheibe auf eine neue Position gedreht. Die verbesserte Sicherheit wurde nun erreicht, indem nicht nur eine sondern fünf dieser Rotoren hintereinandergeschaltet wurden. Auch die Kryha-Maschine wurde von Friedman entschlüsselt. Dennoch bildete sie die Grundlage der weiteren Maschinen.[31]

Die Rolle der Verschlüsselung im zweiten Weltkrieg

Im zweiten Weltkrieg wurde eine Vielzahl an unterschiedlichen Verschlüsselungsmaschinen eingesetzt. Im Laufe des ersten Weltkriegs wurden zahlreiche

[29] vgl. SCHMEH 2004 , S. 44 ff
[30] KIPPENHAHN 2006, S. 198
[31] vgl. WRIXON 2006, S. 253 ff; SCHMEH 2004, S. 47 ff

Funksprüche entschlüsselt und dadurch der Kriegsverlauf entscheidend beeinflusst. Während des zweiten Weltkriegs war dementsprechend von Anfang an klar, dass viel von der Sicherheit der übermittelten Nachrichten abhing. Drei dieser eingesetzten Maschinen beeinflussten den Kriegsverlauf entscheidend – die deutsche Enigma, die japanische Purple und die amerikanische SIGABA.[32]

Die vom deutschen Ingenieur Arthur Scherbius entwickelte Enigma (griechisch für „Rätsel“) ist die wohl populärste aller Verschlüsselungsmaschinen. Sie arbeitete ähnlich wie die Kryha, hatte jedoch neben den üblichen Rotoren einen weiteren, die sogenannte Umkehrwalze, welche das Signal ein zweites Mal durch die Vorrichtung schickte. Dies bewirkte eine doppelte Verschlüsselung und führte zu einer höheren Sicherheit:

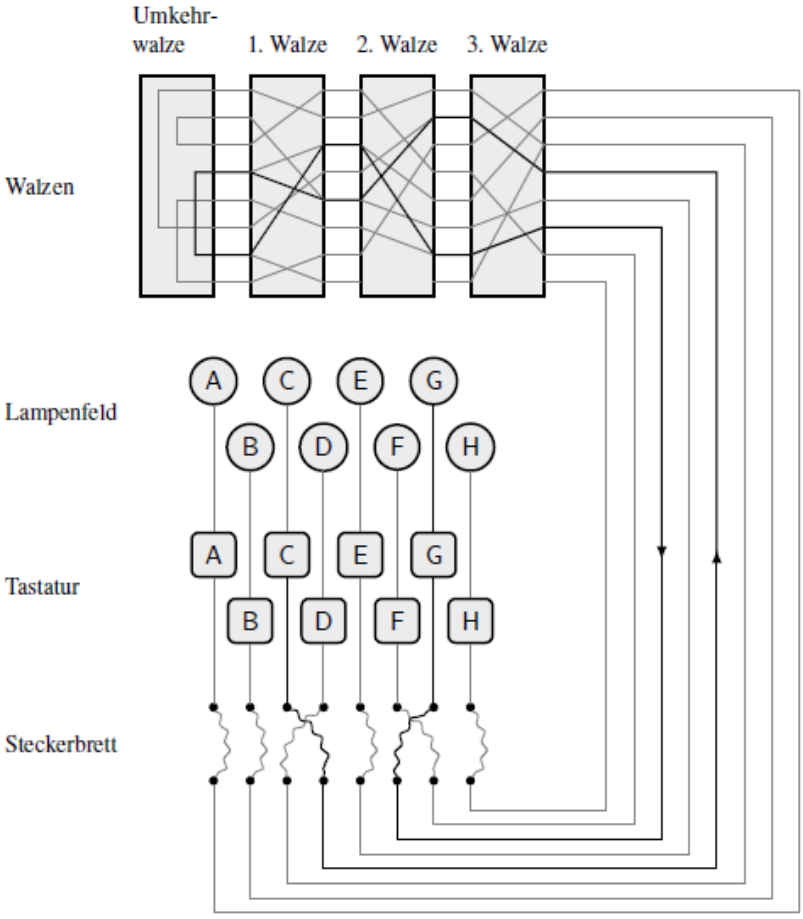

Abbildung 2: Funktionsweise der Enigma[33]

[32] vgl. LUNDE 2009, S. 116 ff
[33] FREIERMUTH u.a. 2010, S. 174

In der obigen Abbildung wird der Buchstabe *C* auf der Tastatur gedrückt und über den Weg durch die Walzen wird ein *G* an den Lampen angezeigt.

Der polnische Abhördienst, der zu dieser Zeit zu den eifrigsten gehörte, konnte lange Zeit nichts mit den abgefangenen Funksprüchen anfangen. Erst als ein französischer Spion Unterlagen und Handbücher lieferte, wussten die Polen, womit sie es genau zu tun hatten. Dennoch konnten sie vorerst keinen Profit aus ihrem Wissen ziehen, da die Anfangsstellungen der Rotoren – also die Schlüssel – nicht bekannt waren. Die Deutschen wechselten diese täglich aus. Durch den zu dieser Zeit einzigartigen Umkehrrotor gelang es den Polen letztendlich doch noch, die Enigma zu entschlüsseln. Sie entwickelten Umkehrmaschinen, mit denen in den Folgejahren hunderttausende Funksprüche entschlüsselt wurden. Die deutsche Enigma wurde jedoch verbessert und um zwei Rotoren erweitert. Mit dieser Veränderung bekamen die Polen Probleme, die sie nicht mehr in den Griff bekamen. So entschieden sie, die verbündeten Geheimdienste der Franzosen und Briten einzuweihen. Wenige Wochen später wurden die Polen überfallen und der zweite Weltkrieg begann.[34]

Die Briten nutzten die Informationen, die sie von den Polen erhielten und entwickelten diese weiter. Es wurden verbesserte Umkehrmaschinen entwickelt, die zur Ermittlung der täglichen Schlüssel eingesetzt wurden. Dennoch wurde es immer schwieriger, diese auch tatsächlich zu finden, da die Deutschen eine Vielzahl an unterschiedlichen Enigma-Maschinen einsetzten und diese stets weiterentwickelten. Letztendlich waren es die eigenen Fehler, die den Deutschen die Funksicherheit kostete. So wurden immer wieder alltägliche Floskeln übermittelt oder es mussten Nachricht erneut übermittelt werden, weil die Funker Fehler machten. Dadurch konnten die Schlüssel um einiges leichter ermittelt werden. Besonders hartnäckig waren die Maschinen der deutschen Marine. Diese Nachrichten erwiesen sich als besonders schwierig zu entschlüsseln. Einerseits, weil die Funker der U-Boote bedeutend weniger Fehler machten und andererseits, weil es sich um eine besonders starke Version der Enigma han-

[34] vgl. LUNDE 2009, S. 120; SCHMEH 2004, S. 63 ff

delte. Die Briten hatten jedoch Glück, als sie 1940 zufällig ein deutsches U-Boot aufbrachen, in dem sich nicht nur eine Enigma sondern auch Schlüsselbücher befanden. Somit konnten monatelang problemlos deutsche Nachrichten entschlüsselt werden.[35]

Die Japaner setzten eine Maschine ein, die nicht mit Rotoren, jedoch nach einem ähnlichen Prinzip funktionierte. Die Purple arbeitete mit Hilfe von elektromechanischen Schaltern, wie sie bei der damaligen Telefonvermittlung eingesetzt wurden. Die Maschine war zwar komplizierter aufgebaut als die Enigma, jedoch gab es weniger mögliche Schlüssel. Die Vorgänger der Purple wurden bereits zuvor durch ein amerikanisches Team rund um William Friedman ohne größere Probleme geknackt. Als die ersten Nachrichten der Purple abgefangen wurden, wurde vermutet, dass es sich um eine verbesserte Version handelte. In der Umbruchsphase kam es dazu, dass die Japaner Nachrichten an mehrere Empfänger versendeten, wobei einige noch nicht mit der Purple sondern mit Vorgängerversionen arbeiteten. Dadurch wusste das Team um Friedman, wie einige verschlüsselte Nachrichten im Klartext aussehen. Obwohl auch die Japaner ähnliche Fehler wie die Deutschen machten, bewegten sich die Fortschritte der Purple-Entschlüsselung nur langsam voran. Nach einem intensiven Jahr hatten die Amerikaner einen Einblick in die Funktionsweise der Purple und machten sich daran, diese nachzubauen. Ein halbes Jahr später konnten die ersten Nachrichten routinemäßig entschlüsselt werden. Die Japaner begnügten sich bei der Schlüsselwahl auf einen Schlüssel, der nur alle zehn Tage vollständig ausgetauscht wurde. Zwischendurch wurde er nach einem bestimmten Schema geändert. Als die Amerikaner dies merkten, wurde die Entschlüsselungsarbeit natürlich um ein Vielfaches erleichtert. So entstand jedoch ein anderes Problem. Es gab zu wenige Leute, die die Sprache beherrschten und loyal genug erschienen, um eingeweiht zu werden und die abgefangenen Nachrichten ins Englische zu übersetzen. Mangelhafte Satzzeichen und viele Fachausdrücke erschwerten diesen Prozess zusätzlich. So dauerte es oft länger eine Botschaft zu übersetzen, als diese zu entschlüsseln. Nach dem Krieg zerstörten

[35] vgl. SCHMEH 2004, S. 72 ff

die Japaner sämtliche Purple–Maschinen, sodass heute keine Exemplare davon mehr existieren. Es gibt lediglich noch drei größere Teilstücke davon.[36]

Ein entscheidender Vorteil

Während sowohl die deutsche Enigma als auch die japanische Purple geknackt wurden, entwickelten die Amerikaner eine Maschine, die nicht geknackt werden konnte. Die SIGABA brachte ihnen dadurch einen entscheidenden Vorteil im Kriegsverlauf. Sie arbeitete mit 15 Rotoren von denen fünf wie bei der Kryha verdrahtet waren. Die anderen zehn dienten der Steuerung und änderten die fünf Verschlüsselungsrotoren mit unregelmäßigen Bewegungen. Die Amerikaner betrieben einen enormen Aufwand um kein Gerät an den Gegner zu verlieren. So wurde eine Maschine, die aktuell nicht gebraucht wurde in drei unterschiedliche Tresore versperrt, sodass Maschine, Rotoren und Schlüsselbücher stets getrennt voneinander aufbewahrt wurden. Dennoch kam ihnen eine Maschine abhanden, als ein unbewachter Transporter vor einem Bordell gestohlen wurde. Es erwies sich jedoch, dass der Dieb – ein Franzose – lediglich Interesse am Fahrzeug hatte. Die Fracht hatte er in einen nahegelegenen Bach geworfen. Die SIGABA wurde weiterhin eingesetzt, bevor sie 1959 ausgemustert wurde. Sie bereitete den Amerikanern auch im Pazifikkrieg gegen die Japaner noch einen sehr großen Vorteil.[37]

In den folgenden Jahren wurden noch zahlreiche andere Verschlüsselungsmaschinen eingesetzt. Auf diese wird hier jedoch nicht weiter eingegangen, da dies den Rahmen der Arbeit sprengen würde. Sie funktionierten zu großen Teilen nach ähnlichen Methoden wie die bereits behandelten Maschinen.

4.4 Verschlüsselung mittels Computer

Um 1970 war die Computertechnik so weit entwickelt, dass sie den Einsatz elektromechanischer Verschlüsselungsmaschinen weitgehend überflüssig

[36] vgl. SCHMEH 2004, S. 84 ff
[37] vgl. SCHMEH 2004, S. 51 ff

machte. Nach und nach stiegen Militär und Geheimdienste auf die neue Technik um. Zur gleichen Zeit begann die Kryptologie eine akademische Disziplin zu werden. Von da an entwickelten sich militärische und öffentliche Verschlüsselungsverfahren, die sich stets wechselseitig beeinflussten. Bis heute hält dieser Fortschritt an, wobei aus Geheimhaltungsgründen stets ungewiss bleiben wird, ob die geheimen militärischen Entwicklungen vielleicht bereits um einiges weiter fortgeschritten sind als die öffentlichen.[38]

Die ersten Computerverschlüsselungen

Am Beginn dieser Epoche stand die Computer-Firma IBM[39], die den damaligen Computermarkt größtenteils dominierte. Es wurde rasch erkannt, dass die Computerdaten geschützt werden mussten. Dabei musste ein Umdenkprozess gegenüber den Verschlüsselungsmaschinen eingeleitet werden, da der Computer nur mit Nullen und Einsen arbeitet. Das erste Verschlüsselungsverfahren, Lucifer, arbeitete mit einem 128 Bit Schlüssel[40] und bediente sich einfacher Bit-Operationen, da diese bereits ein hohes Maß an Sicherheit boten. Im Gegenzug zu einer Vielzahl an unterschiedlichen Bit-Operationen, wurden wenige Operationen dutzendfach angewendet. Dies wird auch bei heutigen Verfahren noch so gehandhabt. Zur gleichen Zeit rief die US-Normierungsbehörde NBS (National Bureau of Standards) zur Einreichung von Vorschlägen für ein taugliches Verfahren auf, das sicher und einfach umzusetzen sein sollte. Das ausgewählte Verschlüsselungsverfahren, Lucifer, wurde eingehend durch den zuständigen Nachrichtendienst, der NSA (National Security Agency), untersucht. Dabei stellte sich heraus, dass dieses Verfahren enorm stark war. Es war sogar so stark, dass die NSA den Schlüssel auf 56 Bit reduzieren lies. Die NSA erhoffte sich, dass das Verfahren in allen zivilen Bereichen zum Einsatz kommt. Die NSA erhoffte sich, dass sie einen Super-Computer bauen können, der

[38] vgl. SCHMEH 2004, S. 197 f

[39] IBM (International Business Machines Corporation) ist ein weltweit führendes IT-Unternehmen aus den USA. IBM beschäftigt sich mit Hardware, Software und auch IT-Dienstleistungen. Es handelt sich heutzutage um eines der größten Beratungsunternehmen und um den zweitgrößten Softwarehersteller weltweit. Entstanden ist IBM 1896 als Unternehmen, das ursprünglich Datenauszählungen mittels Lochkarten durchführte.

[40] Dies bedeutet, dass der Schlüssel in binärer Darstellung eine Länge von 128 Zeichen besitzt. Genauer wird sowohl auf die Zifferndarstellung im Binärsystem, als auch auf die Längen von Schlüsseln in Kapitel 6 (Moderne Kryptographie) eingegangen.

durch Probieren sämtlicher Schlüssel den neuen Code innerhalb kurzer Zeit knacken könnte. Dies hätte der NSA das Mitlesen sämtlicher ziviler Nachrichten und damit eine weitgehende Kontrolle ermöglicht. 1975 veröffentlichte die NBS Lucifer unter dem Namen DES (Data Encryption Standard).

Kryptologen aller Welt nahmen das neue Verfahren unter die Lupe und versuchten erfolglos dieses zu knacken. Dabei galt in diesem Zusammenhang das Knacken eines Codes nicht als anrüchig. Vielmehr waren diese Versuche ein wichtiger Teil der kryptologischen Forschung. Nur durch die Aufdeckung von Schwachstellen konnten diese behoben werden. Mit dem Aufkommen des Internets wurde der DES rasch populär. Sein Einsatzgebiet erstreckte sich von der Absicherung von Geldautomaten bis hin zu der Verschlüsselung von Computerprogrammen. 1990 musste sich das Verfahren einem weiteren Härtetest unterziehen. Adi Shamir[41] entdeckte gemeinsam mit seinem Kollegen Eli Biham die differenzielle Kryptoanalyse – ein neues und sehr machtvolles Verfahren, um einen Code zu knacken. Doch auch hier hielt der DES standhaft dagegen. Bis heute würde er das Verschlüsselungsverfahren schlechthin sein, doch seine kurze Schlüssellänge verhinderte dies. Durch den Zusammenschluss einer Vielzahl von Computern wurden DES-Schlüssel in den Jahren 1997 und 1998 innerhalb von zunächst einigen Tagen, letztendlich innerhalb weniger Stunden geknackt.[42]

Asymmetrische Verfahren

Das Problem des Schlüssels kann jedoch gelöst werden, indem man wieder auf die ursprünglich geplante Schlüssellänge von 128 Bit umsteigt, was auch einige DES-Nachfolger machen. Dennoch gibt es ein Problem, das dem DES Steine in den ansonsten so erfolgreichen Weg legt – der Austausch der Schlüssel. Dieses Problem ist so alt wie die Kryptographie selbst. Es wurde jedoch in den

[41] Adi Shamir (geb. 1952) ist einer der führenden Kryptologieexperten der heutigen Zeit. Der israelische Wissenschaftler wirkte mit der differentiellen Kryptoanalyse und dem RSA-Verfahren an einigen der bedeutendsten Entwicklungen der modernen Kryptologie mit. Weiters hält er Vorträge an einigen hoch angesehenen Universitäten, darunter das MIT, das Weizmann-Institut und die École normal supérieur in Paris.
[42] vgl. SCHMEH 2004, S. 198 ff

siebziger Jahren mit dem asymmetrischen Verschlüsselungsverfahren gelöst. Bei diesem von den beiden amerikanischen Kryptologen Whitfield Diffie und Martin Hellman[43] entdeckten Verfahren können die beiden Kommunikationspartnerinnen bzw. Kommunikationspartner durch einfache Potenzrechnung einen gemeinsamen Schlüssel bestimmen. Eine eventuelle Abhörende bzw. ein eventueller Abhörender kann diesen Schlüssel nur ermitteln, wenn die Potenz-Umkehrung – der Logarithmus – bestimmt werden kann, was jedoch unter bestimmten Voraussetzungen unmöglich ist. Dieses Verfahren bietet heutzutage die Grundlage vieler Verschlüsselungsverfahren und wird millionenfach eingesetzt.[44]

Während Diffie und Hellman noch an ihrem Verfahren arbeiteten, gelang drei anderen Wissenschaftlern der große Durchbruch. Die beiden Informatiker Ron Rivest[45] und Adi Shamir und der Mathematiker Leonard Adleman[46] entwickelten das nach ihnen benannte RSA-Verfahren. Auch dieses basiert auf den Erkenntnissen, die von Diffie und Hellman veröffentlicht wurden. Jedoch handelte es sich bei dem Verfahren nicht um Exponentialfunktionen, sondern um die Multiplikation von sehr großen Primzahlen. Die beiden Primzahlen bilden den privaten Schlüssel, während deren Produkt den öffentlichen Schlüssel ergibt. Auch hier ist die Multiplikation ein einfacher Vorgang, während die Ermittlung der beiden Primfaktoren aussichtslos ist. Voraussetzung dafür ist, dass die gewählten Zahlen ausreichende Länge besitzen. Ihr Verfahren veröffentlichten Rivest, Shamir und Adleman im Jahr 1977. Ähnlich wie beim DES wurde auch das RSA-Verfahren von einer Vielzahl an Experten auf dem Gebiet der Kryptoanalyse untersucht. Dabei wurden Schwachstellen entdeckt, allerdings handelte es sich dabei stets um Spezialfälle. Werden diese vermieden, so ist RSA auch

[43] Die beiden Kryptologieexperten Whitfield Diffie (geb. 1944) und Martin Hellman (geb. 1945) gelten als die Wegbereiter der Public-Key-Kryptographie. Ihre Entwicklungen rund um das Schlüsselaustauschproblem sind die Grundlagen, auf denen bei den Entwicklungen der modernen Verfahren, darunter RSA, aufgebaut wurde.
[44] vgl. SCHMEH 2004, S. 216 ff
[45] Der amerikanische Kryptologe Ronald Linn Rivest (geb. 1947) entwickelte neben dem RSA-Verfahren noch eine Reihe an weiterer Verschlüsselungsmethoden, darunter die Stromchiffren RC2 bis RC6. Weiters war er an der Entwicklung diverse Hash-Algorithmen beteiligt.
[46] Leonard Adleman (geb. 1945) war das prüfende Auge im Entwicklungsteam. Er entdeckte meist die Schwachstellen der entwickelten Verfahren und Methoden – nicht so bei RSA.

heute noch ein sicheres Verfahren. Trotz zahlreicher Weiterentwicklungen konnte keine davon den Erfolgslauf des RSA-Verfahrens bremsen.[47]

Einher mit der Entwicklung asymmetrischer Verfahren ging die Entwicklung der digitalen Signatur. Dabei wird bei der versendeten Nachricht ein spezielles Verfahren angewandt, bei dem auch der private Schlüssel miteinbezogen wird. Der Empfänger kann nun mit Hilfe des zugehörigen öffentlichen Schlüssels den Absender identifizieren. Da der private Schlüssel niemandem außer dessen Besitzer bekannt ist, kann auch niemand eine digitale Signatur imitieren. Die Entwickelung dieses Verfahrens bot erstmals seit 3.500 Jahren eine zweite Anwendung der Kryptologie. Nun gab es nicht nur die Möglichkeit der Verheimlichung einer Nachricht, sondern auch die Verhinderung bei einer versendeten Nachricht einen anderen Absender vorzutäuschen.[48]

Private Nutzung

Durch die Entwicklungen von DES und RSA gab es Anfang der neunziger Jahre genügend Möglichkeiten für den geschäftlichen Datenaustausch. Jedoch gab es diese Möglichkeiten mangels Interesse kaum für den Normalnutzer. Als jedoch die Vernetzung von privaten Computern immer mehr aufkam, änderte sich dies. Dabei entwickelte der Amerikaner Phil Zimmermann im Alleingang ein Verfahren, das zum erfolgreichsten seiner Art wurde – Pretty Good Privacy, kurz PGP – mit dem die Verschlüsselung von E-Mails für jeden ermöglicht werden sollte. Seine Motivation war das wachsende Misstrauen gegen die totale Überwachung durch den Staat. Da Zimmermann allen misstraute, war PGP auch mit keiner anderen Software kompatibel. Dennoch begann durch die freie Verfügbarkeit des Quellcodes und der hohen Sicherheit ein Siegeszug, der bis in die späten neunziger Jahre anhielt.[49]

1997 startete die ehemalige NBS, nunmehr NIST (National Institute of Standards and Technology), einen weiteren Einreichungs-Wettbewerb für ein Ver-

[47] vgl. SCHMEH 2004, S. 220 ff
[48] vgl. SCHMEH 2004, S. 232 ff
[49] vgl. SCHWENK 2010, S. 30 ff

schlüsselungsverfahren. Im Gegensatz zum ersten Wettbewerb, gab es diesmal eine Vielzahl an Teilnehmern. Nach einer fast zweijährigen Überprüfungsphase schieden zehn der 15 Teilnehmer aus. Zwei weitere hatten kaum Siegeschancen, da deren Verschlüsselungsgeschwindigkeit deutlich langsamer waren, als bei den verbleibenden drei. Diese Übriggebliebenen galten allesamt als ebenbürtige Verfahren. Letztendlich setzte sich im Oktober 2000 Rijndael durch, welches von Joan Daemen und Vincent Rijmen eingereicht wurde. Kurze Zeit später wurde es zur neuen offiziellen Verschlüsselungsnorm AES im Behördenbereich der USA.[50]

Das perfekte Verfahren

Ein weiteres Konzept soll hier auch seine Erwähnung finden. Es handelt sich dabei um das One-Time-Pad, dem theoretisch perfekten Verschlüsselungsverfahren. Die ersten Ansätze hierzu waren bereits bei Vigenère zu finden. Eine erste bekannte Realisierung dieses Verfahrens bildete jedoch erst zu Zeiten des Kalten Kriegs das „Rote Telefon“. Streng genommen handelt es sich um eine Erweiterung des Vigenère –Verfahrens, durch den Einsatz eines speziellen Schlüssels. Wenn dieser zwei Kriterien erfüllt, ist das Verfahren nicht zu knacken. Diese beiden Kriterien sind einerseits ein Schlüssel, der genauso lang ist wie die zu verschlüsselnde Nachricht und andererseits die Bedingung, dass jeder Schlüssel nur ein einziges Mal verwendet werden darf. Doch genau diese beiden Kriterien bewirken, dass das Verfahren in der Praxis nicht einfach einsetzbar ist.[51]

Ein vager Blick in die Zukunft zeigt, dass sich auch in den nächsten Jahren im Bereich der Kryptologie einiges tun wird. Ob es die Möglichkeiten von Quanten-Computern, DNA-Computern oder gänzlich anderen Technologien sind – sie werden für weitere Veränderungen und Neuerungen in den Bereichen der Kryptographie und der Kryptoanalyse bringen. Die große Frage die offen bleibt ist, wann dies der Fall sein wird.

[50] vgl. SPITZ u.a. 2011, S. 81; SCHMEH 2004, S. 265 ff
[51] vgl. WRIXON 2006, S. 270 ff

4.5 Die Geschichte der Kryptographie im Schulunterricht

Die geschichtlichen Entwicklungen der Kryptographie bieten umfangreiche Einsatzmöglichkeiten im Schulunterricht. Jede Geschichte kann fesselnd sein, wenn sie gut erzählt wird. Grundlage hierfür ist, dass die Lehrerin bzw. der Lehrer selbst genügend Ahnung von den Geschehnissen hat.

Jedoch bietet die Geschichte nicht nur die Möglichkeiten der Erzählung. Die Ursprünge der Verschlüsselung können mit einfachster Mathematik im Unterricht durchgeführt werden. Durch praktisches Nachvollziehen und Ausprobieren kann die Lehrperson die Schülerinnen und Schüler auf die Schwächen der einzelnen Verfahren hinlenken. Somit erleben diese die Entwicklung und lernen nicht nur darüber.

Der Bereich der Verschlüsselungsmaschinen geht wiederum nur in Richtung eines erzählenden Unterrichts. Ein Nachbauen von Maschinen ist im Unterricht undenkbar. Jedoch kann das Interesse der Schülerinnen und Schüler von der einen oder anderen Geschichte über die Entwicklungen, unterstützt durch Bilder oder Filmausschnitte, geweckt werden. Hier drängt sich ein fächerübergreifender Unterricht zwischen der Informatik und der Geschichte förmlich auf. Auch die Mathematik kann in diesen fächerübergreifenden Unterricht eingebaut werden.

Die computergestützte Verschlüsselung besitzt wiederum mehr Bezug zur Praxis. Hierbei kann der Bezug zu aktuellen Verfahren und Methoden hergestellt werden. Auch wenn die mathematischen Hintergründe teilweise sehr hoch sind, können sie durchaus in einem Oberstufenwahlpflichtfach zumindest teilweise behandelt werden. Beispielsweise kann eine RSA-Verschlüsselung mit verkürzten Schlüssellängen durchaus durchgerechnet werden. Auch eine praktische Vorführung dieser Verfahren ist möglich, was wiederum einen Eindruck über Methoden, Aussehen, Schnelligkeit usw. gibt.

Ein weiteres spannendes Feld ermöglicht das Gebiet der Kryptoanalyse. Die Entschlüsselung von Geheimtexten zeigt oft auf, welche Sicherheitslücken diverse historische Verfahren hatten. Speziell einige händische Verschlüsselungen können durch Schülerinnen und Schüler problemlos geknackt werden. Dabei würde sich die Möglichkeit ergeben Teams zu bilden. Diese erhalten die Aufgabenstellung eine Nachricht nach einem vorgegebenen Verfahren zu verschlüsseln. Anschließend sollen sie versuchen eine Nachricht von einer anderen Gruppe zu knacken. Somit wird einerseits das Verständnis von Verschlüsselungsmethoden weitergegeben, andererseits werden auch das Auffinden von Sicherheitslücken und die Methoden der Kryptoanalyse geschult.

5 Klassische Kryptographie

5.1 Einleitung

Die klassischen Verschlüsselungsverfahren bilden ein Thema, das für den Schulunterricht in mehrfacher Hinsicht nutzbar ist. Zum einen handelt es sich bei den meisten Verfahren um solche, die durch Schülerinnen und Schüler eines Wahlpflichtfaches Mathematik, ohne größere Probleme zu haben, nachvollziehbar sein sollten. Dabei kann das Unbekannte und Rätselhafte daran Interesse wecken, was im Schulunterricht, gerade aber in der Mathematik, einen wichtigen Punkt darstellen sollte. Auf der anderen Seite ist es so, dass zu jedem neuen Themenbereich ein Zugang gefunden werden muss. Natürlich kann die Kryptographie, wie so vieles Andere, einfach präsentiert werden. Dennoch ist es besser, sie zu erfahren. Genau dazu können die klassischen Verfahren herangezogen werden. Obwohl alle diese Verfahren geknackt wurden, können in ihnen dennoch einige wichtige Grundideen der Kryptographie erkannt werden. Aus diesem Grund sind sie nicht nur historisch interessant, sondern mit ihrer Hilfe können auch wichtige Grundlagen für moderne Verfahren vermittelt werden.[52]

5.2 Monoalphabetische Verschlüsselung

Bei monoalphabetischen Verschlüsselungen wird ein Buchstabe des Klartextes auf einen bestimmten anderen Buchstaben abgebildet. Das wohl bekannteste monoalphabetische Verschlüsselungsverfahren ist das Cäsar-Verfahren. Dieses zählt zu den Verschiebungs-Chiffren, bei denen die Reihenfolge der Buchstaben im Alphabet unverändert bleibt, jedoch beginnt dieses Alphabet nicht bei „a“, sondern bei einem anderen Buchstaben. Mathematisch gesehen handelt es sich bei einer Verschiebungs-Chiffre um eine lineare Kongruenz. Die Verschlüsselung kann also dargestellt werden als

[52] vgl. WÄTJEN 2008, S. 13

$M \rightarrow (M + K) \bmod 26$.[53]

Im folgenden Beispiel wird der Klartext „`kryptographie`“ mit dem Schlüssel 6 mittels Verschiebungs-Chiffre verschlüsselt. Aus dem ersten Buchstaben „k“ wird der Buchstabe, der sich im Alphabet um 6 Buchstaben verschoben ist, also „q“. Aus dem Buchstaben „r“ wird der Buchstabe „x“. Das „y“ wird ebenfalls um 6 Buchstaben verschoben. Da dadurch ein Wert erreicht wird, der größer als 26 ist, muss wieder bei „a“ zu zählen begonnen werden. Der verschlüsselte Buchstabe lautet also „e“. Mit den verbleibenden Buchstaben wird analog verfahren. Das verschlüsselte Wort lautet „`qxevzumxgvnok`“. Vereinfachend wird nicht zwischen Groß- und Kleinschreibung unterschieden. Speziell für den Unterricht sollte auch auf Umlaute, Sonderzeichen und Satzzeichen verzichtet werden.

Cäsar in der Schule

Interessant für den Schulunterricht ist diese Verschlüsselungsmethode in mehrfacher Hinsicht. Auf der einen Seite handelt es sich historisch gesehen um eines der ersten Verfahren und bildet damit einen guten Einstieg in die Thematik. Auf der anderen Seite handelt es sich bei diesem Verfahren um eines, das sehr einfach verstanden werden kann und kaum mathematische Grundlagen voraussetzt. Ein Themengebiet wird dennoch behandelt, das in der Schule in dieser Form im Lehrplan nicht vorgesehen ist – die linearen Kongruenzen.[54] Diese können jedoch einfach erklärt werden. Je nachdem auf welchem Leistungsniveau sich die Schülerinnen und Schüler befinden, können die linearen Kongruenzen tatsächlich als solche eingeführt und behandelt werden, oder diese werden nicht explizit erläutert. Der Umgang mit linearen Kongruenzen wird für Mathematiklehrerinnen und Mathematiklehrer im Folgenden vorausgesetzt und wird aus diesem Grund hier nicht weiter behandelt. Weiters eignet sich dieses Verschlüsselungsverfahren sehr gut als Programmierbeispiel, falls der ASCII-Code im Informatikunterricht behandelt wird.

[53] vgl. MATTHES 2003, S. 107
[54] vgl. BMUKK 2004a; BMUKK 2004b; BMUKK 2004c

Wird der Cäsar-Code im Schulunterricht behandelt, können die Schülerinnen und Schüler versuchen die verschlüsselten Texte von ihren Kolleginnen und Kollegen zu knacken. Hierbei werden sie vermutlich recht rasch merken, dass es maximal 26 Versuche braucht, um den Geheimtext entschlüsselt zu haben. Diese geringe Sicherheit kann zur Überleitung zu einem anderen monoalphabetischen Verschlüsselungsverfahren genutzt werden – dem multiplikativen Verschlüsselungsverfahren. Bei dieser Methode werden die Zeichen nicht um den Schlüssel *K* verschoben, sondern mit diesem multipliziert. Multiplizieren bedeutet dabei, dass die Buchstaben auf ihre jeweilige Stelle im Alphabet abgebildet werden. Diese Werte werden anschließend mit dem Schlüssel *K* multipliziert (mod 26). Abschließend erfolgt die Umformung auf den entsprechenden Buchstaben. Beispielsweise wird bei einem Schlüssel $K = 7$ der Buchstabe „k“ zunächst auf den Wert *11* abgebildet. Anschließend erfolgt die Multiplikation mit dem Schlüssel: $11 \cdot 7 = 77$. Modulo *26* ergibt sich nun der 25ste Buchstabe des Alphabets, also ein „y“.

Dabei muss jedoch noch darauf geachtet werden, dass die Kardinalität des Alphabets (üblicherweise 26) und der Schlüssel teilerfremd sind, da ansonsten keine bijektive Abbildung entsteht. Stattdessen werden einige Buchstaben des Alphabets öfters „getroffen“, während auf andere gar nicht abgebildet wird. Diese mehrfachen Treffer bewirken, dass eine eindeutige Umkehrung nicht mehr möglich ist. Anhand von Beispielen kann dies recht rasch demonstriert werden. Vielmehr ist es wahrscheinlich jedoch sinnvoll anhand von Beispielen die Schülerinnen und Schüler zu dieser Notwendigkeit hinzuführen. So könnten die Schülerinnen und Schülern eine Verschlüsselung mit einem Schlüssel aus *{2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24}* durchführen. Ziel ist, dass sie erkennen, dass oben genanntes Problem auftritt. Beispielsweise werden die Klartextbuchstaben bei einem Schlüssel $K = 2$ wie folgt abgebildet:

Klartext:	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Geheim:	a	c	e	g	i	k	m	o	q	s	u	w	y	a	c	e	g	i	k	m	o	q	s	u	w	y

Es kann erkannt werden, dass sich die Buchstaben im Geheimtext ab der Hälfte wiederholen. Eine ähnliche Situation entsteht bei den anderen Schlüsselwerten, die nicht zur Kardinalität des Alphabets teilerfremd sind. Die multiplikative Verschlüsselung kann mathematisch als

$$M \rightarrow (M \cdot K) \bmod 26$$

dargestellt werden.[55] Der Klartext „`kryptographie`“ würde mit dem Schlüssel 7 zu „`yvshjawvghdki`“ verschlüsselt werden.

Wird die Schlüsselmenge betrachtet, die für das multiplikative Verschlüsselungsverfahren in Frage kommt, so wird schnell klar, dass es noch weniger Möglichkeiten gibt als bei der Verschiebechiffre. Es gibt lediglich zwölf Schlüssel die eingesetzt werden können, da nur diese teilerfremd zur 26 sind. Eine Aufgabenstellung für die Schülerinnen und Schüler an dieser Stelle könnte es sein, diese zwölf möglichen Schlüsselwerte herauszufinden. Diese Schwäche kann ausgebessert werden, wenn auf beliebige monoalphabetische Verschlüsselungen erweitert wird. Hierbei werden alle Buchstaben zu jeweils einem beliebigen, aber fest gehaltenen, anderen Buchstaben verändert. Dies kann im Allgemeinen nicht mehr durch eine mathematische Funktion dargestellt werden. Stattdessen werden Tabellen verwendet, in denen steht, welcher Buchstabe worauf abgebildet wird. Damit gibt es eine Vielzahl an möglichen Verschlüsselungen. Genauer gesagt gibt es *26!* verschiedene Möglichkeiten. Hiervon muss noch eine Möglichkeit, nämlich die identische Permutation, abgezogen werden, da es sich dabei um den Klartext und nicht um eine Verschlüsselung handelt. Diese Anzahl kann nun nicht mehr bzw. nur mit enorm hohem Aufwand durch probieren geknackt werden. Ebenfalls gibt es noch eine Vielzahl an monoalphabetischen Verfahren, bei denen der Klartext nicht auf Buchstaben, sondern auf Symbole und Zeichen abgebildet wird. Damit ergibt sich praktisch gesehen eine unendliche Anzahl an möglichen Verschlüsselungen.[56]

[55] vgl. ERTEL 2007, S. 31 f
[56] vgl. WRIXON 2006, S.172 ff

Häufigkeitsanalyse

Jedoch kann den Schülerinnen und Schülern eine Methode erläutert werden, die jede monoalphabetische Verschlüsselung knacken kann. Der große Nachteil von diesen ist nämlich, dass derselbe Klartextbuchstabe stets zum selben Geheimtextsymbol verschlüsselt wird. In jeder Sprache gibt es Tabellen mit Häufigkeitsanalysen, die angeben, welche Buchstaben in dieser Sprache mit welcher Wahrscheinlichkeit auftreten. Für die deutsche Sprache sind die Vorkommen in der folgenden Abbildung ersichtlich.

Buchstabe	Häufigkeit	Buchstabe	Häufigkeit
a	6,51%	n	9,78%
b	1,89%	o	2,51%
c	3,06%	p	0,79%
d	5,08%	q	0,02%
e	17,40%	r	7,00%
f	1,66%	s	7,27%
g	3,01%	t	6,15%
h	4,76%	u	4,35%
I	7,55%	v	0,67%
j	0,27%	w	1,89%
k	1,21%	x	0,03%
l	3,44%	y	0.04%
m	2,53%	z	1,13%

Abbildung 3: Buchstabenhäufigkeit der deutschen Sprache[57]

Die Häufigkeit eines Vorkommens ändert sich bei der Verschlüsselung nicht. Es ändern sich lediglich die Symbole. Dadurch ist es mit hoher Wahrscheinlichkeit so, dass, bei Klartexten der deutschen Sprache, das am häufigsten auftretende Geheimtextsymbol dem „e“ entspricht. Handelt es sich um eine Verschiebechiffre, genügt dieses Wissen bereits um den Schlüssel und damit den gesamten Klartext zu bestimmen. Andernfalls können über die nachfolgenden Buchstaben und über die Häufigkeitstabellen von Buchstabenpaaren und Buchstabentripel weitere Klartextbuchstaben den Symbolen zugeordnet werden. Der erhaltene

[57] BEUTELSPACHER 2009, S. 10

Lückentext kann im Normalfall recht einfach zu dem ursprünglichen Klartext ergänzt werden.[58]

Entschlüsselung anhand eines Beispiels

Ein Beispiel zur Entschlüsselung einer Cäsar-Chiffre wird im Folgenden durchgeführt. Der abgefangene Geheimtext lautet

```
kplzpzalpurbyglyaleaklytpaalsztvuvhswohilapzjolyclyzj
osblzzlsbunjopmmyplyadbyklkbyjokplohlbmpnrlpazhuhsfzl
rhuuklyohlbmpnzalibjozahillytpaalsadlyklukhkbyjodpykk
lyjvkllluazjosblzzlsa
```

Dabei wurden Sonderzeichen und Leerstellen entfernt. Tatsächlich werden diese ebenfalls verschlüsselt. Nun wird eine Häufigkeitsanalyse durchgeführt, bei der die Buchstaben gezählt werden. In der Praxis wird solch ein Vorgang mit Hilfe eines Computers durchgeführt. Hierzu gibt es einige Java-Applets[59], mit denen dies im Unterricht vorgeführt werden kann. Bei einem kurzen Text, so wie hier, kann dies aber durchaus auch händisch geschehen. Die Häufigkeitsanalyse ergibt, dass das Symbol „l“ mit 16,76% vor den Buchstaben „a“ und „y“ mit jeweils 8,38% das häufigste Vorkommen ist. Wie in Abbildung 1 ersichtlich, ist das „e“ mit Abstand der am häufigsten vorkommende Buchstabe im deutschen Alphabet. Nun wird der mögliche Schlüssel gebildet. Der Abstand der Buchstaben „e“ und „l“ beträgt 7. Durch diesen Schlüssel würde sich folgender Klartext ergeben.

```
diesisteinkurzertextdermittelsmonoalphabetischerversch
luesselungchiffriertwurdedurchdiehaeufigkeitsanalyseka
nnderhaeufigstebuchstabeermitteltwerdendadurchwirdderc
odeentschluesselt
```

Wie erkennbar ist, handelt es sich um einen sinnvollen Text. Der abgefangene Geheimtext wurde erfolgreich entschlüsselt, obwohl dieser eine recht kurze Länge hatte.

[58] vgl. ERTEL 2007, S. 34; KÜSTERS & WILKE 2011, S. 34 ff
[59] vgl. Anhang A

Mittels Häufigkeitsanalyse können monoalphabetische Verschlüsselungen also im Allgemeinen recht gut geknackt werden. Hierzu können unterschiedlichste Übungsaufgaben und Beispiele herangezogen werden. Der interessanteste Fall wird jedoch derjenige sein, in dem Schülerinnen und Schüler Nachrichten von ihren Kolleginnen und Kollegen knacken sollen. Dennoch sollte auf jeden Fall klar gemacht werden, dass es sich bei dem Verfahren der Häufigkeitsanalyse nicht um einen garantierten Lösungsweg handelt. Speziell bei sehr kurzen Texten ist die Gefahr auf einen Irrweg zu geraten sehr hoch, da in diesem Fall die Häufigkeiten durch die unzureichende Länge nicht aussagekräftig genug sind. Ebenso können die Häufigkeiten verzerrt sein. Beispielsweise wird es wohl einige Zeit dauern, bis die verschlüsselte Version von „Zwischen zwei Zwetschgenzweigen sitzen zwei zwitschernde Schwalben“ geknackt werden kann. In diesem Beispiel kommen die Buchstaben „z“ und „w“ nämlich überdurchschnittlich häufig vor, was zu einer atypischen Häufigkeitsverteilung führt. Diese bereitet beim Entschlüsselungsversuch Probleme.

5.3 Transpositionsverschlüsselung

Im Gegensatz zu den gerade behandelten monoalphabetischen Substitutionschiffren ändern Transpositionsverschlüsselungen die Buchstaben nicht. Sie verschlüsseln, indem sie die Positionen der Buchstaben vertauschen. Es handelt sich also bei dem erhaltenen Codewort um eine Permutation des Klartextes. Dabei gibt es eine Vielzahl an möglichen Transpositionsvorschriften. Eine historisch interessante Transpositionsverschlüsselung bildet die Skytale. Bei ihr handelt es sich um das erste bekannte kryptographische Werkzeug und zugleich um eine der ersten Transpositionsformen. Dabei wurde Papyrus um einen Stab mit einem bestimmten Durchmesser gerollt. Hierauf wurde anschließend der Klartext verfasst. Durch Abrollen des Papyrusstreifens ergab sich eine andere Reihenfolge der Buchstaben. Dieser Geheimtext konnte nur wieder les-

bar gemacht werden, wenn ein Stab mit gleichem Durchmesser vorhanden war.[60]

Im Laufe der Jahre fanden viele verschiedene Transpositionschiffren ihre Anwendung. Die große Sicherheit solcher Verfahren besteht darin, dass die Entschlüsselung, ohne zu wissen welches Verfahren genutzt wurde, enorm schwierig ist. Es könnte sich jede denkbar mögliche Permutation bei der Verschlüsselung ergeben. Allein für den Klartext „`kryptographie`“ gibt es bereits über 1,5 Milliarden mögliche Permutationen. Eine Kryptoanalyse ist hier ohne Zusatzinformation beinahe unmöglich. Es sollte wenigstens die Thematik des verschlüsselten Textes bekannt sein, um mögliche Irrwege auszuschließen. So könnte es sich bei einer abgefangenen Nachricht, in der eine Permutation des obigen Klartextes vorkommt, auch um den Text „`herr yoga kippt`“ oder um die Worte „`krieg rot happy`“ handeln. Beide Varianten könnten in deutschen Texten vorkommen. Da es sich im Allgemeinen jedoch nicht um eine willkürliche Permutation des Klartextes handelt, sondern um eine Vertauschung der Buchstaben nach einem bestimmten Schema, können auch diese Methoden kryptoanalytisch entschlüsselt werden. Das Verfahren, das hier zum Einsatz kommt nennt man Anagrammieren. Dabei werden die Buchstaben durch Umstellen in die richtige Reihenfolge gebracht.[61]

Transposition in der Schule

Für den Schulunterricht eignen sich diese Verfahren ebenfalls. Einerseits zeigen sie eine neue Möglichkeit neben den Substitutionschiffren auf. Andererseits kann hier das Wissen über Permutationen angewandt werden. Arbeiten die Schülerinnen und Schüler an diesen Verschlüsselungsmethoden, werden sie relativ rasch auch auf den großen Nachteil stoßen. Transpositionsverschlüsselung ist im Vergleich zu anderen Verfahren mühsam umzusetzen. Durch die Geheimhaltung des Verfahrens, muss mit jedem Kommunikationspartner eine eigene Variante vereinbart werden, nach der die Buchstaben vertauscht wer-

[60] vgl. WRIXON 2006, S. 134
[61] vgl. WÄTJEN 2008, S. 13 f

den. Allein hier ist sichtbar, dass es sich nicht um eine Verschlüsselung handelt, die massenweise einsetzbar ist. Weiters liegt das Geheimnis einer Verschlüsselung im genutzten Verfahren. Dies steht im Widerspruch zum Kerkhoffschen Prinzip[62], welches bereits in Kapitel 3 (Grundlagen) erläutert wurde. Ist das Verfahren bekannt, so kann jeder Geheimtext mit geringem Aufwand in den zugehörigen Klartext übergeführt werden. Somit ist dieses Kapitel, wie auch die geschichtliche Entwicklung zeigt, eine Sackgasse der Kryptographie. Dennoch sind auch hier die Erkenntnisse für modernere Verschlüsselungsverfahren von Interesse. Auch ist es wichtig, Schülerinnen und Schülern die Grenzen und Nachteile von Methoden aufzuzeigen.

5.4 Polyalphabetische Verschlüsselung

Im Gegensatz zu monoalphabetischen Verschlüsselungen werden die Buchstaben des Klartextes bei polyalphabetischen Verschlüsselungen nicht stets auf jeweils dasselbe Symbol abgebildet. Die Buchstaben des Klartextes werden auf unterschiedliche Symbole abgebildet. Dadurch werden statistische Häufigkeiten verschleiert. Damit wird die große Schwachstelle von monoalphabetischen Verschlüsselungen behoben.

Homophone Verschlüsselung

Zu den Vertretern der polyalphabetischen Verschlüsselungen zählen die homophonen Chiffren. Hierbei werden die Buchstaben, die mit höherer Wahrscheinlichkeit vorkommen, auf mehrere Symbole abgebildet. So wird beispielsweise das „e“, das in der deutschen Sprache mit einer Wahrscheinlichkeit von etwa 17,4% vorkommt, auf 17 verschiedene Symbole abgebildet, die alle etwa gleich oft verwendet werden. Im Gegenzug dazu werden die Buchstaben „p“ oder „z“ auf jeweils ein einziges Symbol abgebildet. Dadurch ergibt sich für die Verteilung der Geheimtextsymbole nahezu eine Gleichverteilung. Die Dechiffrierung wird dadurch etwas erschwert, jedoch können einzelne Buchstaben, die nicht

[62] vgl. SCHMEH 2004, S. 13 f

eindeutig entschlüsselt werden können, aus der Sinnhaftigkeit der Wörter wiedergewonnen werden.[63]

Nun sieht es auf den ersten Blick so aus, als ob dadurch die Schwachstelle beseitigt wäre und homophone Verschlüsselungen für die Praxis geeignet wären. Tatsächlich ist es so, dass eine Häufigkeitsanalyse der einzelnen Buchstaben nun nicht mehr möglich ist. Jedoch ist es so, dass die unterschiedlichen Buchstabenpaare immer noch mit unterschiedlichen Wahrscheinlichkeiten auftreten. Somit können auch homophone Verfahren mittels Häufigkeitsanalyse geknackt werden, auch wenn hierfür mehr Ressourcen benötigt werden.[64]

Das ist es auch, was den Schülerinnen und Schülern klar gemacht werden kann. Ein Austesten und Erproben wird den Rahmen des Unterrichts vermutlich überschreiten. Dennoch ist das Verständnis dafür ein Ziel, das erreicht werden sollte. Bei der Suche nach weiteren Verfahren, könnte das folgende Verfahren durchaus als Schülerinnen- oder Schülervorschlag auftreten. Die Verknüpfung eines Klartextes mit einem Schlüsselwort ist in Anlehnung an die monoalphabetische Cäsar-Chiffre durchaus gut zu erarbeiten.

Verschiebechiffre

Die Vigenère-Verschlüsselung ist als Erweiterung der Cäsar-Verschlüsselung einfach zu erklären. Anstatt die Buchstaben des Klartextes wie bei der Cäsar-Chiffre jeweils um eine feste Anzahl an Stellen zu verschieben, wird diese Anzahl variiert. Dabei wird ein Verschlüsselungswort verwendet, dessen Buchstaben jeweils für eine Anzahl an Verschiebungen stehen. Nun wird das erste Zeichen des Klartextes mit dem ersten Zeichen des Codewortes verschlüsselt, das zweite Klartextzeichen mit dem zweiten Codewortzeichen und so weiter. Wird das Ende des Verschlüsslungswortes erreicht, so beginnt dieses wieder beim Anfang. Um diese Verschlüsselungsvorschrift zu verbildlichen, kann ein Vigenère-Quadrat gebildet werden. Ein solches ist in der unten stehenden Abbildung zu sehen. Hierbei wird nun der jeweilige Geheimtextbuchstabe ermittelt,

[63] vgl. MATTHES 2003, S. 108; ERTEL 2007, S. 35 f
[64] vgl. ERTEL 2007, S. 36

indem die Zeile des Klartextbuchstaben mit der Spalte des Schlüsselbuchstaben geschnitten wird. Das erhaltene Symbol ist der verschlüsselte Buchstabe.[65]

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

Abbildung 4: Das Vigenère-Quadrat[66]

Ein Beispiel soll die Vigenère-Codierung verdeutlichen. Die Verschlüsselung des Klartextes „`kryptographie`“ mit dem Schlüsselwort „`geheim`“ ergibt den Geheimtext „`qvftbamvhtpuk`“.

M: *k r y p t o g r a p h i e*

K: *g e h e i m g e h e i m g*

C: *q v f t b a m v h t p u k*

[65] vgl. MATTHES 2003, S. 109 f; WÄTJEN 2008, S. 37 f
[66] FREIERMUTH u.a. 2010, S. 102

Wie die historische Entwicklung zeigt, ist ein Geheimtext der mittels Vigenère verschlüsselt wurde, nicht unbedingt auf den ersten Blick zu knacken. Dennoch gibt es eine Methode, die im Schulunterricht so erläutert werden kann, dass sie für die Schülerinnen und Schüler verständlich ist. Es handelt sich bei diesem Entschlüsselungsverfahren um den Kasiski-Test. Bevor dieser im Unterricht bearbeitet wird, sollte eine Motivationsphase stattfinden. Hierbei ist es wichtig zu verstehen, dass eigentlich nicht die Unkenntnis des Schlüssels das Hindernis bei der Entschlüsselung bildet. Vielmehr genügt es, bei einem ausreichend langen Geheimtext die Länge des Schlüssels zu kennen. In diesem Fall kann der codierte Text in Teilblöcke zerlegt werden. Diese Teilstücke sind nun, wie bei der Cäsar-Chiffre, monoalphabetisch verschlüsselt, was wiederum durch Häufigkeitsanalysen geknackt werden kann. Spätestens, wenn die Schülerinnen und Schüler selbst eine Nachricht mittels Vigenère verschlüsselt haben, sollte das Verständnis hierfür gegeben sein.

Der Kasiski-Test knackt Vigenère

Nun stellt sich noch die Frage, wie die Schlüssellänge ermittelt werden kann. Hier kommt der Kasiski-Test ins Spiel. Dieser basiert auf einer einfachen Beobachtung. Gleiche Buchstabenkombinationen im Originaltext werden, wenn diese um ein Vielfaches der Schlüssellänge auseinander liegen, wiederum zu gleichen Buchstabenfolgen im Geheimtext. Dies bedeutet also, dass im Geheimtext nach gleichen Buchstabenfolgen gesucht wird. Von diesen muss jeweils der Abstand notiert werden. Dabei werden üblicherweise nur Buchstabenfolgen untersucht, die zumindest die Länge drei besitzen, da es ansonst zu viele Vorkommen wären. Nun wird der größte gemeinsame Teiler der Abstände gebildet. Dabei kann es vorkommen, dass eventuelle Ausreißer, also Buchstabenfolgen, die sich zufällig wiederholen, zunächst aussortiert werden müssen. Diese Ausreißer können zu Irrwegen und Sackgassen beim Austesten führen. Üblicherweise, wird mit Buchstabenfolgen möglichst großer Länge gearbeitet. Diese deuten meist auf ganze Wörter hin, die sich im Text wiederholen. Der

erhaltene größte gemeinsame Teiler ist nun ein heißer Kandidat für die Schlüssellänge und damit für die Anzahl an Teiltexten.[67]

In der Praxis wird der Kasiski-Test über den Computer durchgeführt. Diverse Hochschulen stellen hierfür Java-Applets[68] zur Verfügung. Mit diesen kann der Kasiski-Test im Schulunterricht demonstriert und durchgeführt werden. Die händische Bearbeitung ist ebenfalls möglich. Der Zeitaufwand für solch eine Entschlüsselung sollte jedoch nicht unterschätzt werden.

Ein Beispiel zur Kryptoanalyse

Im Folgenden wird ein Beispiel zum Knacken eines Geheimtextes, welcher mittels Vigenère-Verschlüsselung codiert wurde dargestellt. Im Unterricht muss dabei, wie bei allen kryptoanalytischen Aufgabenstellungen, darauf geachtet werden, dass die Geheimtexte eine ausreichende Länge für einen Angriff besitzen. Der abgefangene Text, der geknackt werden soll lautet

```
fwhwkgwikbnytnhvvsaxfsuqkhwingymisqitsyitgflnihwusoxyi
uhgrxvevgipydwkgnmvsvxmoqrfwhwevoyggvinzdipuhitalxvsox
ysuhgbgepoflmchrpsqhkswikzwizhhqkhwingkewtlkmslxuoqenm
vidsdvdslxghzitrhrucnsgbqiprlilszikzlkgbkewtlkuhhrdifl
uhdfgbeiuhlqohzitrhrwseitrlidifluhdfgbyithhmniqkmoqrfo
qeevgitxhagwomisdfuhdrfklidslhgffeggdvxsuwevoyggviniqk
dsvxkapxysuhgbcynswdvklvfrhvispikbveosvgjzxiughpdsvxka
pxwbghgffsfshrvgflnihwusoxz
```

Im ersten Schritt muss mittels Kasiski-Tests herausgefunden werden, welche Buchstabenfolgen sich wiederholen. Von diesen Abständen wird im Anschluss der größte gemeinsame Teiler bestimmt, welcher mit großer Wahrscheinlichkeit die gesuchte Schlüssellänge ist. Im obigen Geheimtext finden sich die folgenden wiederholenden Buchstabenfolgen. Dabei wurden nur Folgen berücksichtigt, die mindestens fünf Buchstaben lang sind.

[67] vgl. KÜSTERS & WILKE 2011, S. 38 f; ERTEL 2007, S. 38 ff
[68] vgl. Anhang A

`gflnihwusox` (Länge 11)	352 Zeichen Abstand
`difluhdfgb` (Länge 10)	32 Zeichen Abstand
`wevoyggvin` (Länge 10)	228 Zeichen Abstand
`dsvxkapx` (Länge 8)	48 Zeichen Abstand
`qkhwing` (Länge 7)	116 Zeichen Abstand
`hzitrhr` (Länge 7)	56 Zeichen Abstand
`xysuhgb` (Länge 7)	224 Zeichen Abstand
`kewtlk` (Länge 6)	56 Zeichen Abstand
`moqrf` (Länge 5)	188 Zeichen Abstand

Nun wird der größte gemeinsame Teiler der unterschiedlichen Abstände ermittelt.

ggT (32, 48, 56, 116, 188, 224, 228, 352) = 4

Somit ist eine mögliche Schlüssellänge bestimmt. Also wird ein Schlüsselwort mit vier Buchstaben gesucht. Dies bedeutet, dass der Geheimtext in vier Teiltexte unterteilt werden muss, wobei jeder vierte Buchstabe zum selben Teilblock gehört. Von diesen werden nun mittels Häufigkeitsanalyse die Buchstaben bestimmt, die jeweils am häufigsten vorkommen. Ähnlich wie bei der monoalphabetischen Cäsar-Verschlüsselung kann hierdurch der entsprechende Codebuchstabe ermittelt werden. Für den ersten Teiltext

```
fkktvfknittnuygepkvmfegnptvygpmpkkzknwmunddgtugplkgwud
uguotwtdugtnmfetgiufdggxegndkygnvfikojudkwgfvnuz
```

ergibt die Häufigkeitsanalyse, dass der Buchstabe „g“ mit knapp 14% der häufigste ist. Dieser besitzt den Abstand 2 zu „e“. Das bedeutet, dass der erste Buchstabe des Schlüssels ein „c“ ist. Analog kann mit den anderen drei Teiltexten verfahren werden. Dies ergibt für den zweiten Teiltext

```
wgbnsshgssgisirvygsowvgzuassbocsszhhgtsomsshrcbrszbthi
hbhhrsrihbhioovxwshksfgsvgisasbskrsbszgsabfsgis
```

den Buchstaben „s“ mit über 25% als häufigsten und damit den Schlüsselbuchstaben „o“. Für den dritten Teiltext

```
hwnhauwyqyfhouxgdnvqhovdhlougfhqwwhwkllqvdlzhnqlzlklhf
delzhelfdyhqqqghoddllfduovqvpucwlhpvvxhvpgfhfho
```

ist das „h“ mit mehr als 15% der häufigste Buchstabe. Dies ergibt den Schlüsselbuchstaben „d“. Für den letzten Teiltext

```
wiyvxqimiilwxhviwmxrwyiiixxhelrhiiqiekxeivxirsiiikekrl
fiqiriilfimkreiamfrihevwyikxxhydvviegipxxhsrlwx
```

ist das „i“ mit über 25% der häufigste Buchstabe. Dadurch ergibt sich hier das „e“ als Schlüsselbuchstabe. Der erhaltene Schlüssel im Beispiel lautet also „`code`“. Mit diesem Schlüsselwort wird nun der Geheimtext entschlüsselt. Tatsächlich entsteht ein Text, der Sinn ergibt. Damit ist der verschlüsselte Text geknackt.

```
diesisteinkurzertextdermittelsvigenereverschluesseltwu
rdedurchdenkasiskitestkanndieschluessellaengeermittelt
werdendanachkoennendieteiltextemittelshaufigkeitsanaly
sebearbeitetwerdensokoennendiejeweiligenhaufigstenbuch
stabenbestimmtwerdenueberdiebuchstabenverteilungkannda
nachderjeweiligeabstandwiebeidercaesarverschluesselung
bestimmtwerdenzuletztwirddergemeinsameschluesselbestim
mtunddercodeentschluesselt
```

6 Moderne Kryptographie

6.1 Einleitung

Als die Computer Ende der 1980er Jahre weit genug entwickelt waren, lösten sie die elektromechanischen Verschlüsselungsmaschinen nach und nach ab. Dies hatte zur Folge, dass neue Methoden entwickelt werden mussten. Da der Computer im Kommunikationswesen vorerst nicht mehr wegzudenken ist, sind auch die in diesem Kapitel behandelten Verschlüsselungsverfahren zu großen Teilen noch heute im Einsatz.

Hierbei sollen zunächst Alice, Bob und Eve Erwähnung finden. Diese sind die wohl bekanntesten „Menschen" der modernen Kryptologie. Sie tauchen in der Literatur immer wieder auf und stehen symbolisch für die verschiedenen Kommunikationspartnerinnen und Kommunikationspartner. In der Vergangenheit wurde von „Person A", „Person B", „Person C" und so weiter gesprochen. In den siebziger Jahren wurden daraus die fiktiven Personen Alice und Bob, welche die Kommunikationspartnerinnen und Kommunikationspartner darstellen und Eve, die die Angreiferin bzw. den Angreifer darstellt.[69]

ASCII

Die Darstellung von Buchstaben im Computer erfolgt üblicherweise mittels ASCII-Code[70]. Hierbei wird jedem Symbol eine Dezimalzahl zugeordnet, die folgender Abbildung entnommen werden kann:

[69] vgl. LUNDE 2009, S. 274 f

[70] Der American Standard Code for Information Interchange (ASCII) ist eine Codierungsmethode für Zeichensätze. Entwickelt wurde dieser 1963. Dabei wurden die codierten Darstellungen für 128 Zeichen definiert. Es handelt sich bei diesen Zeichen weitgehend um diejenigen, die auf einer englischen Tastatur zu finden sind. Der ursprüngliche Standard codierte die Zeichen in eine 7-Bit-Binärfolge. Ein achtes Bit wird bei zahlreichen Erweiterungen eingesetzt um sprachspezifische Zeichen ebenfalls codieren zu können – beispielsweise Umlaute in der deutschen Sprache.

ASCII	Zeichen	ASCII	Zeichen	ASCII	Zeichen
32	(Leer)	64	@	96	`
33	!	65	A	97	a
34	"	66	B	98	b
35	#	67	C	99	c
36	$	68	D	100	d
37	%	69	E	101	e
38	&	70	F	102	f
39	'	71	G	103	g
40	(	72	H	104	h
41	)	73	I	105	i
42	*	74	J	106	j
43	+	75	K	107	k
44	,	76	L	108	l
45	-	77	M	109	m
46	.	78	N	110	n
47	/	79	O	111	o
48	0	80	P	112	p
49	1	81	Q	113	q
50	2	82	R	114	r
51	3	83	S	115	s
52	4	84	T	116	t
53	5	85	U	117	u
54	6	86	V	118	v
55	7	87	W	119	w
56	8	88	X	120	x
57	9	89	Y	121	y
58	:	90	Z	122	z
59	;	91	[	123	{
60	<	92	\	124	|
61	=	93	]	125	}
62	>	94	^	126	~
63	?	95	_	127	DEL

Abbildung 5: ASCII-Tabelle[71]

Auf die Auflistung der ersten 32 Zeichen (von 0 bis 31) wurde in dieser Abbildung verzichtet, da es sich dabei um Steuerzeichen handelt, denen üblicherweise in der Kryptologie keine Bedeutung zukommt. Um nun tatsächlich eine Vorstellung davon zu erhalten, wie mit diesen Zeichen gearbeitet wird, sollte zunächst das binäre Zahlensystem[72] behandelt werden. Nun kann mit Hilfe der obigen Tabelle beispielsweise die Binärdarstellung des Buchstaben *k* gebildet werden, also die Form, mit der der Computer tatsächlich arbeitet. Dazu muss die Dezimalzahl *107* umgewandelt werden. Die binäre Darstellung würde *0110 1011* lauten. Da der Umgang mit Binärzahlen für den Computer einfach

[71] LUNDE 2009, S. 273
[72] Das Binärsystem (auch Zweiersystem oder Dualsystem) nutzt zur Darstellung von Zahlen nur die Ziffern 0 und 1. Aufgrund seiner Bedeutsamkeit in der Digitaltechnik ist es neben dem Dezimalsystem das zweitwichtigste Zahlensystem der heutigen Zeit.

ist, für den Menschen allerdings unübersichtlich sein kann, erfolgt die Angabe häufig im Hexadezimalsystem[73]. Aus diesem Grund finden sich in den Tabellen häufig auch diese Angaben und die Schülerinnen und Schüler sollten auch damit vertraut gemacht werden. Die hexadezimale Darstellung für den Buchstaben *k* lautet beispielsweise $6B = 6 \cdot 16^1 + 11 \cdot 16^0$.

Die XOR-Operation

Zu den wichtigsten Operationen für binäre Zahlen zählt die XOR-Operation. Als Symbol für diese Operation wird in weiterer Folge $\oplus$ verwendet. Die Operation wird für einige moderne Verschlüsselungsverfahren genutzt, weshalb sie im Unterricht zunächst als Grundlage behandelt werden sollte. Dabei ist sie denkbar einfach. Falls die beiden Bits, welche mittels XOR verknüpft werden, übereinstimmen, ist das Ergebnis eine *0*. Stimmen die beiden Bits nicht überein, ist das Ergebnis eine *1*. Die XOR-Verknüpfung entspricht also der Addition Modulo 2. Bei mehrstelligen Binärzahlen, wird die Operation bitweise durchgeführt. Voraussetzung ist, dass beide Zahlen die gleiche Länge aufweisen.[74]
Ein Beispiel hierfür wäre:

$$\begin{array}{r} 1001\ 1010\ 1001\ 0101 \\ \underline{\oplus\ 0111\ 1011\ 0101\ 0110} \\ 1110\ 0001\ 1100\ 0011 \end{array}$$

6.2 Data Encryption Standard (DES)

Eines der ersten modernen Verschlüsselungsverfahren ist unter dem Namen DES bekannt. Dabei handelt es sich um ein Block-Chiffrierverfahren, bei dem die binär dargestellte Nachricht in Blöcken der Länge 64 Bit verschlüsselt wird. Im ersten Schritt muss die Nachricht in solche Teile zerlegt werden. Diese Blöcke werden nun alle nach dem gleichen Schema verschlüsselt. Die Verschlüs-

[73] Das Hexadezimalsystem nutzt zur Darstellung von Zahlen die Basis 16. Neben den Ziffern von 0 bis 9 werden hierfür die Buchstaben von A (=10) bis F (=15) genutzt. Aufgrund der einfachen Umformung zum Binärsystem – eine hexadezimale Ziffer entspricht genau einer Vierergruppe in der binären Darstellung – wird das Hexadezimalsystem häufig als komfortablere Darstellung für dieses eingesetzt.
[74] vgl. SCHNEIER 2006, S. 15 f

selung läuft in drei Schritten ab – der Eingangspermutation, der Rundenverschlüsselung und der Abschlusspermutation. Im ersten Schritt erfolgt die Eingangspermutation. Diese ordnet die 64 vorhandenen Bits nach dem folgenden Schema neu an. Dabei geben die abgebildeten Zahlen die Reihenfolge an, in der die Bits sortiert werden. Das 58ste der 64 Bits wird also an die erste Stelle gesetzt, das 50ste kommt an die zweite Stelle, das 42ste an die dritte Stelle und so weiter.[75]

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Abbildung 6: Eingangspermutation[76]

Das folgende Beispiel soll die erste Phase des DES näher erläutern. Der Klartext „`kryptologie`“ soll verschlüsselt werden. Hierzu wird zunächst aus der obigen ASCII-Tabelle die interne Darstellung ermittelt. Die Dezimaldarstellung der einzelnen Buchstaben

107 114 121 112 116 111 108 111 103 105 101

wird in die zugehörige hexadezimale Darstellung umgewandelt. Es ergibt sich

6B 72 79 70 74 6F 6C 6F 67 69 65.

Nun soll nur der erste 64-Bit-Block verschlüsselt werden. Also wird nur noch mit

6B 72 79 70 74 6F 6C 6F

weitergearbeitet. Mit den weiteren Blöcken einer Nachricht wird analog verfahren. Nun erfolgt die Eingangspermutation, nach der obigen Darstellung. Dies könnte mit den Schülerinnen und Schülern in der Schule einmal händisch durchgeführt werden. Die weiteren Permutationen sollten dann jedoch eher mit einem der zahlreichen Programmen, die im Internet[77] verfügbar sind, durchgeführt werden.

[75] vgl. SCHNEIER 2006, S. 316; DORNINGER 2004, S. 109
[76] SCHNEIER 2006, S. 317
[77] vgl. Anhang A

Die Binärdarstellung der Nachricht

01101011 01110010 01111001 01110000

01110100 01101111 01101100 01101111

wird permutiert zu

11111111 00011110 11110000 10100101

00000000 11111111 11100101 10100011.

Die Rundenverschlüsselung

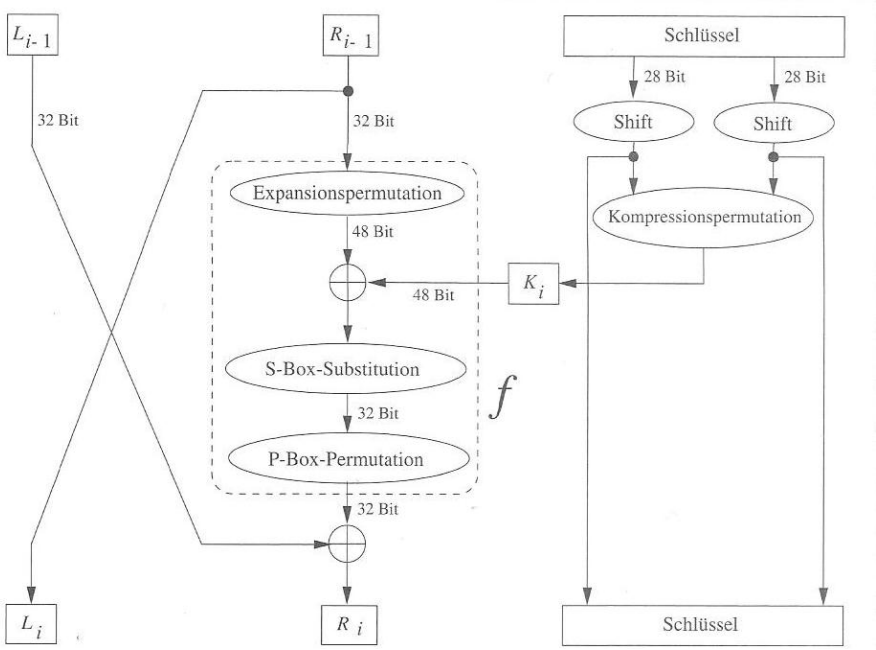

Abbildung 7: Ablauf von jeder der 16 Verschlüsselungsrunden[78]

Nach dieser ersten Permutation erfolgen 16 Verschlüsselungsrunden, welche stets nach folgender Darstellung ablaufen. Nach der Eingangspermutation wird der 64-Bit-Block in eine linke und eine rechte Hälfte – *L* und *R* – geteilt. Im obigen Beispiel ergibt die obere Zeile die linke Hälfte und die untere Zeile die rechte Hälfte für den weiteren Ablauf. Nach jeder Verschlüsselungsrunde wird die linke Hälfte durch die unveränderte rechte Hälfte ersetzt ($L_i = R_{i-1}$), während die

[78] ERTEL 2007, S. 63

neue rechte Hälfte aus einer Reihe von Operationen entsteht. Wie dies genau geschieht wird im Folgenden erläutert.[79]

Die erste von fünf Operationen um die neue rechte Seite zu erhalten ist die Expansionspermutation. Hierbei wird die alte rechte Hälfte von 32 Bit auf 48 Bit erweitert, also expandiert. Zudem werden die Bits noch in eine andere Reihenfolge gebracht. Die neue Reihenfolge ist der folgenden Abbildung zu entnehmen. Hauptzweck dieses Schrittes ist es, den Teil des Klartextes auf dieselbe Länge zu bringen, die auch der Schlüsselteil hat, mit dem in weiterer Folge verknüpft wird.

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

Abbildung 8: Expansionspermutation[80]

Im obigen Beispiel wird die rechte Seite

00000000 11111111 11100101 10100011

mit Hilfe der Expansionspermutation zur Bitfolge

10000000 00010111 11111111 11110000 10111101 00000110

expandiert. Spätestens in dieser Phase sollte von der händischen Arbeit auf die Arbeit mit dem Computer umgestiegen werden, da sonst nur unübersichtliche binäre Zahlenfolgen entstehen. Aus diesem Grund wird auch hier das obige Beispiel nicht weiter geführt.

Der Schlüssel

Im nächsten Schritt werden die erhaltenen Bits mit den entsprechenden Bits des Schlüssels verknüpft. Die durchgeführte Verknüpfung in diesem Schritt ist die zuvor beschriebene XOR-Operation. Bevor diese jedoch stattfinden kann,

[79] vgl. ERTEL 2007, S. 63
[80] SCHNEIER 2006, S. 319

müssen die jeweiligen Schlüsselteile generiert werden. Hierzu wird der 64-Bit-Gesamtschlüssel zunächst auf 56 Bit reduziert, indem jedes achte Bit gestrichen wird. Zudem erfolgt auch hier eine Permutation, die Schlüsselpermutation, welche in der folgenden Abbildung zu sehen ist.

57	49	41	33	25	17	9	1	58	50	42	34	26	18
10	2	59	51	43	35	27	19	11	3	60	52	44	36
63	55	47	39	31	23	15	7	62	54	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Abbildung 9: Schlüsselpermutation[81]

Anschließend wird für jede der 16 Runden ein unterschiedlicher Teilschlüssel geformt. Diese besitzen jeweils eine Länge von 48 Bit und werden generiert, indem der zunächst 56 Bit lange Gesamtschlüssel in zwei Teile geteilt wird, die jeweils 28 Bit lang sind. Je nach Runde werden diese beiden Teile für sich um ein oder zwei Bits verschoben und anschließend mit der sogenannten Kompressionspermutation zum Teilschlüssel für die aktuelle Runde zusammengefügt. Durch die Verschiebung entsteht für jede Runde ein anderer Teilschlüssel. Sowohl die Verschiebung, als auch die Permutation sind in den folgenden Abbildungen zu finden.[82]

Runde	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Anzahl	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Abbildung 10: Schlüsselverschiebung[83]

14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Abbildung 11: Kompressionspermutation[84]

[81] SCHNEIER 2006, S. 318
[82] vgl. SCHNEIER 2006, S. 318
[83] SCHNEIER 2006, S. 318
[84] SCHNEIER 2006, S. 318

S-Box und P-Box

Nun erfolgt der nächste Teil der Verschlüsselung. Dieser trägt den Namen S-Box-Substitution. Dabei werden die aktuellen 48 Bit in Blöcke zu je 6 Bit geteilt, von denen jeder auf einen 4-Bit-Block reduziert wird. Es entsteht also eine Reduktion auf 32 Bit. Hierzu gibt es für jeden Block eine 4x16 Matrix aus der die entsprechenden ausgehenden Bits ermittelt werden. Dabei geben das erste und das letzte Bit eines eingehenden Blocks die Zeile der Matrix an und die anderen vier Bits geben die Spalte an. Am entsprechenden Feld steht eine 4 Bit lange Zahl, welche dem Ergebnis entspricht.[85]

	Spalte																
Zeile	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S_6
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S_7
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S_8
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

Abbildung 12: S-Box Substitution des DES[86]

Nun erfolgt die P-Box-Permutation, durch welche die 32 Bit erneut in eine andere Reihenfolge gebracht werden:

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Abbildung 13: P-Box Permutation[87]

[85] vgl. WÄTJEN 2008, S. 50 f
[86] WÄTJEN 2008, S. 53

Der letzte Schritt einer Runde ist die Verknüpfung der erhaltenen 32-Bit-Folge mit der unveränderten linken Hälfte. Der so entstandene Teil ist nun für die nächste Runde die rechte Hälfte.[88]

Abschlusspermutation

Nachdem die zuvor beschriebenen Schritte für alle 16 Runden durchgeführt wurden, wird die erhaltene codierte Binärfolge ein letztes Mal permutiert. Diese Schlusspermutation ist invers zur Eingangspermutation. Das bedeutet, dass beispielsweise das Bit, welches zu Beginn an die erste Stelle verschoben wurde, nun wieder an die 40ste Stelle gesetzt wird.[89]

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

Abbildung 14: Schlusspermutation[90]

Um nun eine Nachricht, welche mittels DES verschlüsselt wurde, wieder lesbar zu machen, genügt es, die oben beschriebenen Schritte erneut auszuführen. Jedoch muss die Reihenfolge etwas abgeändert werden. Genauer gesagt wird mit der Schlusspermutation gestartet. Anschließend erfolgen die 16 Runden in umgekehrter Reihenfolge. Abschließend erfolgt die Eingangspermutation.[91]

DES in der Schule

Dieses Verfahren bietet im Schulunterricht einen guten Einstieg in die Verschlüsselung mittels Computer. Die einzelnen Teile des Gesamtkonzepts sollten auf jeden Fall zunächst anhand von kleineren Beispielen erläutert und händisch bearbeitet werden, wobei hier nicht alle Schritte bearbeitet werden müssen, da diese stets nach demselben Schema funktionieren. Eine Behandlung

[87] SCHNEIER 2006, S. 321
[88] vgl. ERTEL 2007, S. 63
[89] vgl. WÄTJEN 2008, S. 50
[90] SCHNEIER 2006, S. 323
[91] vgl. PAAR & PELZL 2010, S. 69 ff

wie im obigen Beispiel sollte für die händische Bearbeitung ausreichend sein. Eine gesamte Verschlüsselung per Hand durchzuführen ist wohl zu umfangreich. Jedoch gibt es anschauliche Seiten im Internet[92], mit denen der DES demonstriert werden kann.

Da beim DES die Sicherheit einzig und allein in der Geheimhaltung des Schlüssels liegt, erfüllt er in dieser Hinsicht zwar die Anforderungen moderner Verschlüsselungsverfahren, wie sie nach dem Kerkhoffschen Prinzip, welches bereits in Kapitel 3 (Grundlagen) behandelt wurde, gefordert werden. Durch die Kombination von Permutationen und Substitutionen bietet der DES auch große Sicherheit gegen eine Vielzahl von Angriffen. Allerdings ist die Anzahl der möglichen Schlüssel mit 2^{56} nach heutigem Stand der Technologie zu klein um ausreichende Sicherheit zu bieten. Dennoch besitzt das Verfahren mit seiner sehr schnellen Verschlüsselungsgeschwindigkeit einen großen Vorteil. Aus diesem Grund wird es auch heutzutage noch vielfach eingesetzt, beispielsweise bei Geldausgabeautomaten oder bei der Sprachverschlüsselung, allerdings meist in einer erweiterten Variante, dem Triple-DES. Hierbei wird die Verschlüsselung drei Mal hintereinander mit jeweils unterschiedlichen Schlüsseln durchgeführt, wodurch sich der mögliche Schlüsselraum deutlich erhöht.[93]

6.3 Diffie-Hellman

Bei vielen modernen Verschlüsselungsverfahren, wie auch beim DES, liegt die Sicherheit im Schlüssel. Dies bedeutet einerseits, dass dieser Schlüssel gut gewählt und geheim gehalten werden muss. Andererseits bildet dies auch ein neues Problem. Wie sollen sich die Teilnehmerinnen und Teilnehmer einer Kommunikation einen gemeinsamen Schlüssel ausmachen? Eine Lösung hierfür entwickelten Whitfield Diffie und Martin Hellman 1976 mit ihrem Verfahren.

[92] vgl. Anhang A
[93] vgl. ECKERT 2004, S. 320 f

Die Schlüsselvereinbarung

Um den gemeinsamen Schlüssel zu erzeugen, einigen sich Alice und Bob auf eine sehr große Primzahl *p*. Wie eine solche Zahl gefunden werden kann, wird in Kapitel 6.7 (Primzahltests) behandelt. Weiters wählen die beiden eine Zahl *x* für die gilt, dass sie im Bereich *{2, 3, …, p-2}* liegt. Diese beiden Zahlen müssen nicht geheim gehalten werden. Alice und Bob können sie also problemlos vereinbaren.

Nun erfolgt die eigentliche Schlüsselvereinbarung. Hierzu wählt Alice eine weitere Zahl *a* aus dem Bereich *{2, 3, …, p-2}* und berechnet damit

$$A \equiv x^a \bmod p.$$

Bob wählt ebenfalls eine Zahl *b* aus diesem Bereich und bildet damit

$$B \equiv x^b \bmod p.$$

Nun tauschen die beiden die erhaltenen Zahlen A und B aus. Alice bildet nun

$$B^a \equiv (x^b)^a \equiv x^{ab} \bmod p$$

während Bob

$$A^b \equiv (x^a)^b \equiv x^{ab} \bmod p$$

bildet. Die beiden haben nun einen gemeinsamen Schlüssel bestimmt.[94]

Anhand eines Beispiels mit kleinen Zahlen, kann dieser Vorgang auch in der Schule erläutert werden. Alice und Bob einigen sich auf $p = 29$ und $x = 2$. Alice wählt die Zahl $a = 5$ und bildet $2^5 \equiv 3 \bmod 29$. Bob wählt hingegen die Zahl $b = 12$ und bildet $2^{12} \equiv 7 \bmod 29$. Nun tauschen die beiden ihre berechneten Zahlen aus und bilden den gemeinsamen Schlüssel. Alice erhält $7^5 \equiv 16 \bmod 29$ während Bob $3^{12} \equiv 16 \bmod 29$ erhält. Der gemeinsame Schlüssel $k = 16$ kann nun für eine verschlüsselte Übertragung genutzt werden.[95]

[94] vgl. BEUTELSPACHER u.a. 2010, S. 28 ff
[95] vgl. PAAR & PELZL 2010, S. 207

Sicherheit des Verfahrens

Nun stellt sich die Frage, warum Eve nicht an den Schlüssel gelangen kann. Würde Eve die Übertragung bei der Schlüsselvereinbarung abhören, so wären ihr *x, p, A* und *B* bekannt, nicht aber der Schlüssel *k*. Dieser könnte nur berechnet werden, indem a und b durch Auflösen der Gleichungen

$$A \equiv x^a \bmod p \qquad \text{und} \qquad B \equiv x^b \bmod p$$

ermittelt werden. Würde es sich um Gleichungen in den reellen Zahlen handeln, wäre das Auflösen mittels Logarithmus kein Problem. Durch die Modulo-Operation wird dieser Vorgang jedoch erheblich erschwert. Bei einer sehr groß gewählten Primzahl p, ist es nahezu unmöglich diese Gleichungen zu lösen. Dies wird das Problem des diskreten Logarithmus genannt. Zu beachten ist jedoch, dass bislang lediglich kein anderes Verfahren für die Lösung dieses Problems bekannt ist. Es ist nicht bewiesen, dass es nicht irgendwann eine Möglichkeit zur Lösung dieser Kongruenzen gibt.[96]

6.4 RSA

Der wohl bekannteste Vertreter von asymmetrischen Verschlüsselungsverfahren – also Verfahren bei denen ein anderer Schlüssel für die Chiffrierung verwendet wird, als für die Dechiffrierung – ist das RSA-Verfahren. Es zählt heutzutage zu den meistgenutzten Verfahren. Anders als bei symmetrischen Verfahren, wie beispielsweise dem DES, wird beim RSA-Verfahren statt eines einzelnen Schlüssels *k* zur Ver- und Entschlüsselung ein Zahlenpaar *(e, n)*, das den öffentlichen Schlüssel bildet, benötigt. Mit diesem werden Nachrichten verschlüsselt, die an eine Empfängerin bzw. einen Empfänger versendet werden sollen. Dazugehörend wird ein zweites Zahlenpaar *(d, n)*, welches den privaten Schlüssel bildet, gebraucht. Mit diesem kann die verschlüsselte Nachricht wieder entschlüsselt werden. Aus diesem Grund muss dieses Paar, genauer gesagt die Zahl *d*, geheim gehalten werden.[97]

[96] vgl. ECKERT 2004, S. 424 f
[97] vgl. MATTHES 2003, S. 158 f; SONNENSCHEIN 2011, S. 10 ff

Ermittlung der Schlüsselpaare

Natürlich sind *e, d* und *n* keine beliebigen Zahlen. Diese müssen nach bestimmten Regeln gebildet werden. Hierfür müssen zunächst zwei möglichst große Primzahlen *p* und *q* gefunden werden (vgl. Kapitel 6.7 - Primzahltests). Aus diesen wird das Produkt $n = p \cdot q$ gebildet, welches Teil beider Schlüssel ist. Nun muss *d* so gewählt werden, dass es kleiner als *n* ist und die Bedingung $ggT(d, \varphi(n)) = 1$ erfüllt, wobei $\varphi(n) = (p - 1) \cdot (q - 1)$. Üblicherweise wird hierfür ein *d* gewählt, welches zwischen $max(p, q)$ und $\varphi(n) - 1$ liegt. Weiters wird nun *e* ermittelt, welches ebenfalls kleiner als *n* sein muss. Außerdem soll die Bedingung $e \cdot d \equiv 1 \bmod \varphi(n)$ erfüllt sein. In der Praxis wird *e* über den erweiterten euklidischen Algorithmus[98] ermittelt. Dieser Vorgang wird anschließend anhand eines Beispiels noch erläutert. Sobald die Schlüsselpaare ermittelt worden sind, sollten die beiden Primzahlen *p* und *q* verworfen werden, da mit diesen durch eine Außenstehende oder einen Außenstehenden ein Rückschluss auf die Schlüssel gezogen werden könnte. Verworfen bedeutet dabei, dass die beiden Werte, da sie nicht mehr benötigt werden, eliminiert werden können. Sie sind natürlich dennoch unbedingt geheim zu halten.[99]

Ein erstes einfaches Beispiel

Mit den beiden Primzahlen $p = 7$ und $q = 11$ kann die Schlüsselpaarermittlung in der Schule per Hand berechnet werden. Das Produkt ergibt $n = 7 \cdot 11 = 77$ und $\varphi(n) = 6 \cdot 10 = 60$. Nun soll $d = 13$ gewählt werden. Dies erfüllt die Bedingung $ggT(d, \varphi(n)) = 1$, wie mit Hilfe des euklidischen Algorithmus gezeigt werden kann:

$$60 = 4 \cdot 13 + 8$$
$$13 = 1 \cdot 8 + 5$$
$$8 = 1 \cdot 5 + 3$$
$$5 = 1 \cdot 3 + 2$$
$$3 = 1 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

[98] vgl. CZAKLER 2007, S. 21 ff
[99] vgl. ECKERT 2004, S. 331; EISLER 2008, S. 39 f

Der Rest *1* in der vorletzten Zeile zeigt, dass tatsächlich $ggT(d, \varphi(n)) = 1$ gilt. Über rückwärtiges Einsetzten kann *e* ermittelt werden:

$$
\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (5 - 1 \cdot 3) = -5 + 2 \cdot 3 \\
&= -5 + 2 \cdot (8 - 1 \cdot 5) = 2 \cdot 8 - 3 \cdot 5 \\
&= 2 \cdot 8 - 3 \cdot (13 - 1 \cdot 8) = -3 \cdot 13 + 5 \cdot 8 \\
&= -3 \cdot 13 + 5 \cdot (60 - 4 \cdot 13) = 5 \cdot 60 - 23 \cdot 13
\end{aligned}
$$

Hieraus ergibt sich:

$1 \bmod 60 \equiv -23 \cdot 13$ und damit $13^{-1} \bmod 60 \equiv e = 37.$

Es entstehen also die beiden Paare *(13, 77)* als öffentlicher Schlüssel und *(37, 77)* als privater Schlüssel. Die Primzahlen $p = 7$ und $q = 11$ werden verworfen.[100]

Ein weiteres Beispiel zur Schlüsselpaarermittlung

Ein weiteres Beispiel, jedoch mit größeren Zahlen soll im Folgenden behandelt werden. Dabei empfiehlt es sich, die Berechnungen mit Hilfe eines CAS, wie beispielsweise Maple, durchzuführen. Es werden die beiden Primzahlen $p = 61$ und $q = 97$ gewählt. Dadurch ergibt sich für $n = 61 \cdot 97 = 5917$ und für $\varphi(n) = 60 \cdot 96 = 5760$. Der Wert $d = 1103$ erfüllt die Bedingung $ggT(d, \varphi(n)) = 1$, wie folgende Berechnung auch zeigen wird. Es wird der größte gemeinsame Teiler von 1103 und 5760 über den euklidischen Algorithmus bestimmt werden:

$$
\begin{aligned}
5760 &= 5 \cdot 1103 + 245 \\
1103 &= 4 \cdot 245 + 123 \\
245 &= 1 \cdot 123 + 122 \\
123 &= 1 \cdot 122 + 1 \\
122 &= 122 \cdot 1 + 0
\end{aligned}
$$

[100] vgl. WÄTJEN 2008, S. 73

Bei dem Rest *1* in der vorletzten Zeile handelt es sich um den größten gemeinsamen Teiler der beiden Zahlen. Die oben geforderte Bedingung $ggT(d, \varphi(n)) = 1$ ist also tatsächlich erfüllt. Nun wird *e* ermittelt. Um dieses zu erhalten wird schrittweise rückwärts eingesetzt:

$$1 = 123 - 1 \cdot 122$$
$$= 123 - 1 \cdot (245 - 1 \cdot 123) = -245 + 2 \cdot 123$$
$$= -245 + 2 \cdot (1103 - 4 \cdot 245) = 2 \cdot 1103 - 9 \cdot 245$$
$$= 2 \cdot 1103 - 9 \cdot (5760 - 5 \cdot 1103) = -9 \cdot 5760 + 47 \cdot 1103$$

Daraus ergibt sich:

$1 \bmod 5760 \equiv 47 \cdot 1103$ und damit $1103^{-1} \bmod 5760 \equiv e = 47.$

Es entstehen also die beiden Paare *(47, 5917)* als öffentlicher Schlüssel und *(1103, 5917)* als privater Schlüssel. Die Primzahlen $p = 61$ und $q = 97$ werden verworfen. In der Praxis wird tatsächlich meist der kleinere der beiden erhaltenen Werte *d* und *e* als öffentlicher Schlüsselteil verwendet. Dies bewirkt, dass die Verschlüsselung der Nachrichten rascher abläuft.[101]

Verschlüsselung einer Nachricht

Jede Kommunikationsteilnehmerin und jeder Kommunikationsteilnehmer ermittelt, wie oben beschrieben, die beiden Schlüsselpaare *(d, n)* und *(e, n)*. Nun werden alle öffentlichen Schlüsselpaare in eine Liste eingetragen, welche jedem zugänglich ist. Möchte Alice nun eine Nachricht an Bob senden, so sucht sie zunächst das öffentliche Schlüsselpaar *(e, n)* von Bob aus der Liste. Anschließend verschlüsselt sie mit Hilfe von diesem Paar ihre Nachricht in folgender Form:

$$C \equiv M^e \bmod n$$

Hierzu muss die als Zahl dargestellte Nachricht in Teilblöcke zerlegt werden, die kleiner sind als *n*. Jeder dieser Teilblöcke wird, wie oben beschrieben, ver-

[101] vgl. ERTEL 2007, S. 82, 167 f

schlüsselt. Die verschlüsselte Nachricht kann nun an Bob gesendet werden. Dieser wiederum benötigt zum Entschlüsseln sein Privatschlüsselpaar *(d, n)*. Mit Hilfe von diesem kann er die einzelnen Teilblöcke durch

$$M \equiv C^d \bmod n$$

entschlüsseln.[102]

Beispiel zur Nachrichtenverschlüsselung

Alice möchte den Klartext „`kryptographie`“ mittels RSA verschlüsseln und an Bob übermitteln. Hierzu sucht sie sich das öffentliche Schlüsselpaar *(47, 5917)* von ihm aus der Liste. Im nächsten Schritt muss der Klartext in seine ASCII-Zeichen umgewandelt werden. Dies ergibt die dezimale Darstellung:

$$M = 107\ 114\ 121\ 112\ 116\ 111\ 103\ 114\ 097\ 112\ 104\ 105\ 101.$$

Nun wird für jeden Block die Verschlüsselung durchgeführt. Diese Berechnungen sollten auch im Schulunterricht jedenfalls mit Hilfe eines CAS erfolgen. Im ersten Fall ergibt sich

$$C_1 \equiv 107^{47} \bmod 5917 = 3618.$$

Werden alle Teile berechnet entsteht die verschlüsselte Nachricht.

$$C = 3618\ 2773\ 5428\ 181\ 1312\ 3000\ 178\ 2773\ 2425\ 181\ 3381\ 1152\ 5214$$

Diese wird nun an Bob übertragen, welcher sie mit seinem privaten Schlüsselpaar entschlüsseln möchte. Hierzu nimmt er jeden Teil und bildet diesen wie zuvor beschrieben wieder auf die ursprüngliche Bedeutung ab. Dadurch erhält er die Ausgangsnachricht von Alice. Die händische Durchführung einer Nachrichtenverschlüsselung im Unterricht kann mit sehr kleinen Zahlen durchaus erfolgen. Für eine Demonstration mit Werten wie im obigen Beispiel können diverse Quellen[103] im Internet herangezogen werden.

[102] vgl. SCHNEIER 2006, S. 533 f
[103] vgl. Anhang A

Sicherheit von RSA

Es wird angenommen, dass die Sicherheit der RSA-Verschlüsselung auf dem Faktorisierungsproblem für große Zahlen beruht. Unter dem Faktorisierungsproblem wird verstanden, dass für zwei sehr große Primzahlen *p* und *q* das Produkt *n* zwar mit dem Computer einfach zu berechnen, die Zerlegung von *n* in seine beiden Primfaktoren jedoch sehr schwierig ist. Dieses Problem besteht bereits seit langer Zeit. Heutzutage gibt es einige Verfahren, mit denen die Primfaktoren einer Zahl bestimmt werden können, wie beispielsweise die Faktorisierungsmethode von Lehman, die Kettenbruchmethode oder die Pollard-Rho-Methode. Auf diese soll hier jedoch nicht näher eingegangen werden. Das Entscheidende an all diesen Methoden ist jedoch, dass der Berechnungsaufwand mit heutiger Technologie für große Zahlen *n* immer noch sehr hoch.[104]

Allerdings handelt es sich auch hierbei nur um eine Annahme, die bisher nicht mathematisch bewiesen werden konnte. Einerseits könnte es sein, dass es eine einfache, noch nicht gefundene, Methode zur Faktorisierung gibt. Andererseits könnte es auch sein, dass zum Entschlüsseln einer verschlüsselten Nachricht *C* die Faktorisierung von *n* auch gar nicht notwendig ist.[105]

Eine Methode zur Faktorisierung

Der einfachste Algorithmus zur Faktorisierung einer Zahl *n* ist das Sieb des Eratosthenes[106]. Hierbei wird versucht, die Zahl *n* durch alle ungeraden Zahlen zu teilen, die kleiner als deren Wurzel sind. Dabei wird der Größe nach die Liste der möglichen Primfaktoren abgearbeitet. Bei jeder Division durch eine Zahl, bei der ein Rest bleibt, kann nicht nur die Zahl selbst, sondern auch alle ihre Vielfachen aus der Liste der möglichen Primfaktoren gestrichen werden. Diese Methode besitzt, so wie alle bekannten Verfahren, einen großen Nachteil. Die Rechenzeit wächst proportional zur Größe von *n*. Andere Verfahren, die zur Faktorisierung eingesetzt werden können, sind ebenfalls für große Zahlen zu lang-

[104] vgl. GOLUCH 2011, S. 50 f; HASIBEDER 2010, S. 6
[105] vgl. ECKERT 2004, S. 327, 336
[106] Eratosthenes von Kyrene (3. Jhdt v. Chr.) war ein vielseitiger griechischer Gelehrter. Er betätigte sich in den Bereichen Mathematik, Geographie, Astronomie, Historik, Philologie, Philosophie und Dichtung.

sam. Dies ist der entscheidende Punkt für die Sicherheit des RSA-Verfahrens.[107]

6.5 Advanced Encryption Standard (AES)

Der AES ist heutzutage das meistgenutzte symmetrische Verschlüsselungsverfahren. Dabei gilt das Verfahren, das eigentlich den Namen Rijndael trägt, als Nachfolger des DES, welcher bereits in Abschnitt 6.2 behandelt wurde. Aktuell gibt es keine bekannte Angriffsmöglichkeit gegen das Verfahren. Allerdings gilt auch hier, dass bislang nicht bewiesen ist, dass es keine Möglichkeiten gibt. Aus heutiger Sicht wird erwartet, dass es sich bei dieser Verschlüsselungsmethode um die dominierende der nächsten Jahrzehnte handeln wird. Der AES ist, wie auch der DES, ein Block- Chiffrierverfahren. Allerdings haben die Blöcke der binär dargestellten Nachricht hier eine Länge von 128 Bit.[108]

Der AES kann mit einer Schlüssellänge von 128, 192 oder 256 Bit arbeiten. Ähnlich wie der DES, gibt es auch hier mehrere Runden bei der Verschlüsselung. Die Anzahl von diesen hängt dabei von der Schlüssellänge ab. Bei einer Schlüssellänge von 128 Bit werden 10 Runden durchgeführt, bei 192 Bit erfolgen 12 Runden und bei einer Schlüssellänge von 256 Bit sind es 14 Runden. Eine Runde besteht aus vier Phasen – einer Substitution, einer Permutation, einer Diffusion und der Verknüpfung mit einem Schlüsselteil.[109]

Um die Funktionsweise des AES verständlich darstellen zu können, eignet es sich, wenn sowohl die Blöcke der Nachricht, als auch der Schlüssel in Form einer Matrix aufgefasst werden. Dabei werden Matrizen mit 4 Zeilen verwendet, wobei jeder Matrixeintrag aus 8 Bit, also einem Byte, bestehen soll. Dementsprechend ergeben sich für die Blöcke der Nachricht 4 Spalten und für den Schlüssel je nach Länge 4, 6 oder 8 Spalten. Weiters sollten für eine einfachere

[107] vgl. ERTEL 2007, S. 83 f, SCHNEIER 2006, S. 336 f
[108] vgl. PAAR & PELZL 2010, S. 87 ff
[109] vgl. ECKERT 2004, S. 323 f

Lesbarkeit die Einträge in hexadezimaler Schreibweise erfolgen. Dies reduziert die Einträge auf zwei Stellen. Im Folgenden soll die Funktionsweise anhand des 128-Bit-Schlüssels erläutert werden.

Schlüsselverknüpfung

Bevor die erste Runde begonnen wird, erfolgt eine XOR-Verknüpfung der Nachricht mit einem ersten Schlüsselteil. Hierzu wird der Schlüssel in mehrere Teile aufgeteilt. Genauer gesagt wird ein Schlüsselteil mehr benötigt, als es Runden gibt, da in jeder Runde ein Teil benötigt wird und zu Beginn ein weiterer. Dazu wird nun der gesamte Schlüssel in 4 Blöcke zu je 32 Bit geteilt. Nun werden rekursiv weitere Blöcke gebildet. Hierfür wird jeweils der vorangegangene Block mit dem Block, der um eine Schlüssellänge (also 4 Blöcke) voranging mittels XOR verknüpft. Somit entsteht also der fünfte Block, indem der vierte und der erste Block verknüpft werden, der sechste Block entsteht durch eine Verknüpfung der Blöcke fünf und zwei und so weiter. Dies wird bis zum 44sten Block fortgesetzt. Nun bilden jeweils vier Blöcke einen Rundenschlüssel der Länge 128 Bit.[110]

Die Rundenfunktion

Im nächsten Schritt erfolgen die eigentlichen Verschlüsselungsrunden. Dabei erfolgt zunächst, ähnlich wie beim DES, eine Substitution mittels S-Box. Hierbei wird jeder Zelleneintrag der Matrix nach der folgenden Abbildung ersetzt. Dabei geben die ersten vier Bit an, in welcher Zeile sich der neue Eintrag befindet und die weiteren vier Bit geben an, in welcher Spalte er steht. Beispielsweise wird der Eintrag *C2* substituiert durch den Eintrag *25*.

[110] vgl. ERTEL 2007, S. 73, PAAR & PELZL 2010, S. 106 ff

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Abbildung 15: S-Box Substitution des AES[111]

Im nächsten Schritt erfolgt eine Permutation. Diese wird über eine Zeilenrotation durchgeführt. Dabei werden die vier Zeilen der Matrix zyklisch nach links verschoben. Dies wird in jeder Zeile so weit durchgeführt, dass die Diagonalelemente an erster Stelle stehen.[112]

Spaltentransformation

Nun werden die Spalten der Matrix transformiert. Um diesen Schritt verstehen und durchführen zu können, werden Berechnungen in Galois-Körpern[113] benötigt. Dies würde vermutlich im Schulunterricht zu weit führen. Aus diesem Grund soll auch hier nicht näher auf diese Transformation eingegangen werden. Den Schülerinnen und Schülern kann jedoch erläutert werden, dass durch diese Spaltentransformation, jeder Eintrag einer Spalte mit jedem anderen Eintrag derselben Spalte in Wechselbeziehung steht. Weiters sollte erwähnt werden, dass dieser Vorgang zwar händisch einiges an Aufwand und Hintergrundwissen benötigt, in der Praxis allerdings sehr einfach über Verschiebungen und XOR-Operationen realisiert werden kann.[114]

[111] KÜSTERS & WILKE 2011, S. 69
[112] vgl. MATTHES 2003, S. 128
[113] Ein Galois-Körper oder auch endliche Körper besteht aus einer endlichen Menge an Elementen und den beiden Operationen Addition und Multiplikation, die auf diesem unter Einhaltung bestimmter Regeln definiert sind. Insbesondere gibt es für jede Primzahl *p* genau einen solchen Körper, den sogenannten Restklassenkörper Modulo p. Diese Körper spielen bei kryptografischen Vorgängen eine große Rolle.
[114] vgl. SCHNEIER 2006, S. 324

Im letzten Schritt einer Runde erfolgt die XOR-Verknüpfung mit dem nächsten Schlüsselteil. Auf diesen Schritt muss hier auch nicht mehr näher eingegangen werden, da er bereits vorab erläutert wurde. Im Folgenden sind die einzelnen Schritte einer Runde schematisch dargestellt:

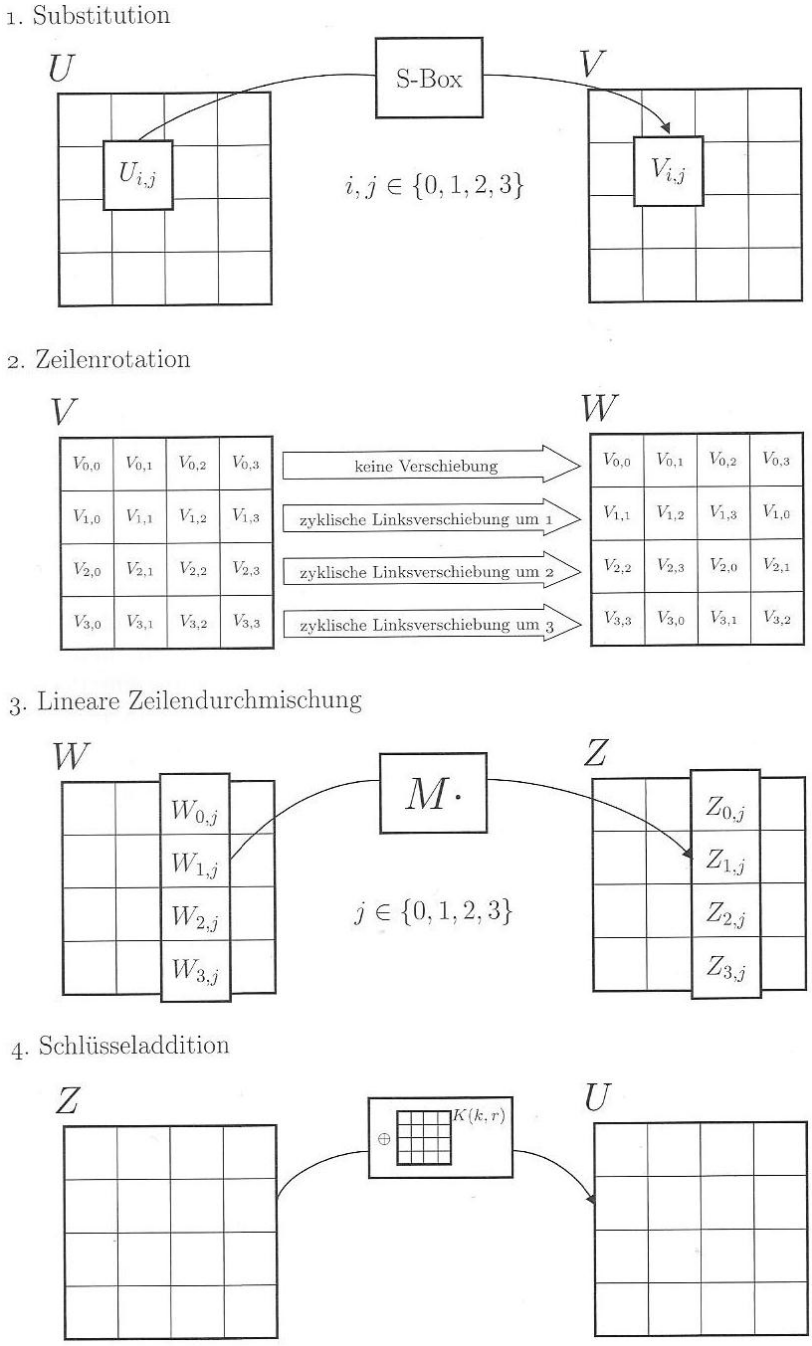

Abbildung 16: reguläre AES-Runde[115]

[115] KÜSTERS & WILKE 2011, S. 70

So werden nun alle Runden bis zur vorletzten abgearbeitet. Die letzte Runde unterscheidet sich von den anderen dahingehend, dass in dieser keine Spaltentransformation stattfindet. Dieser Schritt wird hier weggelassen, weil er ohne Kenntnis des Schlüssels rückgängig gemacht werden könnte.[116]

Um eine Nachricht, welche mittels AES verschlüsselt wurde, wieder lesbar zu machen, müssen einerseits alle Transformationen invertiert werden und andererseits muss die Reihenfolge sämtlicher Verschlüsselungsoperationen umgekehrt werden.[117]

AES im Unterricht

Um den AES im Schulunterricht behandeln zu können wird einiges an Grundwissen vorausgesetzt. Aus diesem Grund können zwar, ähnlich wie beim DES, einzelne Teile anhand kleinerer Beispiele demonstriert und erläutert werden, allerdings wird eine genaue Behandlung der gesamten Funktionsweise den Schulunterricht übersteigen. Eine gesamte Verschlüsselung mittels Hand ist vermutlich nicht realisierbar. Speziell das notwendige Wissen über endliche Körper wird hier ein Problem darstellen. Allerdings kann auch die Verschlüsselung mittels AES zumindest teilweise anschaulich dargestellt werden. Auch hier bietet das Internet[118] unterschiedliche Möglichkeiten. Dennoch sollte in dieser Arbeit nicht auf dieses heutzutage sehr wichtige Verfahren verzichtet werden.

Bezüglich des Themas Sicherheit ist zu erwähnen, dass AES so konstruiert wurde, dass es von keinem bisher bekannten Angriffsverfahren geknackt werden kann. Gleichzeitig wird gehofft, dass auch künftig keine solche Methode entdeckt wird. Das Verschlüsselungsverfahren gilt also nach heutigem Stand als sicher. Da das Verfahren durch eine Vielzahl an Sicherheitskontrollen geschleust wurde, können Nutzer auf dieses Urteil vertrauen. Dennoch wird auch der AES nicht ewig sicher bleiben.[119]

[116] vgl. KARPFINGER & KIECHLE 2010, S. 50
[117] vgl. PAAR & PELZL 2010, S. 110 ff
[118] vgl. Anhang A
[119] vgl. ERTEL 2007, S. 74

6.6 Das theoretisch perfekte Verfahren

Dennoch gibt es ein Verfahren, das zumindest theoretisch perfekte Sicherheit bietet. Es handelt sich beim One-Time-Pad um eine Sonderform der Vigenère-Verschlüsselung, welche bereits in Kapitel 5.4 (Polyalphabetische Verschlüsselung) behandelt wurde. Das Besondere dabei ist, dass die Verschlüsselung mit einem unendlich langen Schlüsselwort durchgeführt wird. In der Praxis bedeutet dies, dass die Länge des Schlüssels größer sein muss als die Länge der zu verschlüsselnden Nachricht. Üblicherweise wird dabei die binär dargestellte Nachricht über eine XOR-Verknüpfung mit dem Schlüssel verknüpft. Die Entschlüsselung erfolgt ebenso wie die Verschlüsselung über eine XOR-Verknüpfung mit demselben Schlüssel.[120]

Die Sicherheit des Verfahrens liegt in der Zufälligkeit der Schlüsselfolge. Diese bewirkt, dass es keine Möglichkeit gibt, aus einer verschlüsselten Nachricht den Klartext rekonstruieren zu können. Dadurch, dass jeder denkbar mögliche Schlüssel eingesetzt werden kann, kann auch der zugehörige Klartext jede denkbar mögliche Form annehmen. Dennoch kommt dieses Verfahren in der Praxis nur in sehr seltenen Fällen zur Anwendung. Der Grund dafür ist, dass die Erzeugung echter Zufallszahlen prinzipiell auf einem Computer nicht möglich ist. Es besteht nur die Möglichkeit Pseudozufallszahlen zu erzeugen. Dies bedeutet allerdings, dass das Verfahren keine ganz perfekte Sicherheit mehr bietet. Doch auch wenn es mit modernen Methoden möglich ist, annähernd Zufallszahlen zu erzeugen, bleibt noch ein weiteres Problem, nämlich der Austausch dieses zufälligen Schlüssels. Hierfür gibt es bislang keine Methode, die einen praktischen Einsatz effizient ermöglicht.[121]

[120] vgl. WRIXON 2006, S. 273 ff, KARPFINGER & KIECHLE 2010, S. 24 f
[121] vgl. ERTEL 2007, S. 53 ff

6.7 Primzahltests

Da bei einigen der behandelten Verfahren sehr große Primzahlen benötigt werden, ergibt sich die Fragestellung, ob eine zufällig gewählte natürliche Zahl prim ist oder nicht. Hierzu werden Algorithmen benötigt, die diese Überprüfung möglichst rasch ermöglichen. Dabei kommen in der Praxis aus Laufzeitgründen üblicherweise keine Algorithmen zum Einsatz, die mit absoluter Sicherheit ein Ergebnis liefern. Vielmehr werden Algorithmen eingesetzt, die mit einer möglichst hohen Wahrscheinlichkeit bestätigen, dass eine zu testende Zahl prim ist. Diese Algorithmen werden Primzahltests genannt. Einige davon sollen im Folgenden behandelt werden.

Fermat-Test

Eine erste Möglichkeit zur Überprüfung, ob eine Zahle prim ist bietet der Fermat-Test[122]. Dieser sollte im Schulunterricht als erster Schritt behandelt werden, weil er die grundlegende Idee der folgenden Tests bildet. Der Fermat-Test basiert auf dem „kleinen Satz von Fermat“, der aussagt, dass für jede zu einer Primzahl *p* teilerfremde natürliche Zahl *a* die folgende Aussage gilt:

$$a^{p-1} \equiv 1 \bmod p.$$[123]

Der entscheidende Schritt hierbei ist, dass die Umkehrung nicht notwendigerweise gelten muss. Der exakte Beweis des Satzes soll hier nicht behandelt werden, kann jedoch beispielsweise bei KARPFINGER & KIECHLE[124] nachgeschlagen werden.

Aus obiger Aussage, kann nun der Fermat-Test abgeleitet werden. Hierbei wird die Testung einer Zahl *n* so durchgeführt, dass zunächst eine Zahl *a* aus dem Bereich *{2, …, n-1}* gewählt wird. Nun wird $a^{n-1} \bmod n$ bestimmt. Diese Berechnung kann mit Hilfe eines Computeralgebrasystems, wie beispielsweise Maple oder Derive sehr einfach durchgeführt werden. Ergibt dies ein anderes Ergebnis

[122] Benannt nach dem französischen Mathematiker des 17. Jahrhunderts Pierre de Fermat, der den zugrundeliegenden Satz formulierte.
[123] vgl. MATTHES 2003, S. 182; REMPE & WALDECKER 2009, S. 74 ff
[124] KARPFINGER & KIECHLE 2010, S. 100

als *1*, so handelt es sich definitiv um eine zusammengesetzte Zahl. Andernfalls könnte es sich um eine Primzahl handeln. Ist der Test nun für viele verschiedene Zahlen *a* erfüllt, so handelt es sich mit hoher Wahrscheinlichkeit um eine Primzahl. Die genaue Wahrscheinlichkeit des Testverfahrens kann nicht bestimmt werden, jedoch steigt diese mit zunehmender Anzahl an Testfällen. [125]

Ein Beispiel zum Fermat-Test

Ein Beispiel soll den Fermat-Test verdeutlichen. Es soll getestet werden, ob die Zahl $n = 341 (= 11 \cdot 31)$ eine Primzahl ist. Im ersten Schritt wird mit $a = 2$ berechnet:

2^{340} *modulo 341.*

Das erhaltene Ergebnis ist *1*, was bedeutet, dass es sich bei *341* eventuell um eine Primzahl handelt. Nun wird im nächsten Schritt $a = 3$ gewählt und berechnet:

3^{340} *modulo 341.*

Das erhaltene Ergebnis in diesem Fall lautet *56*. Die Zahl *341* ist also definitiv keine Primzahl sondern eine zusammengesetzte Zahl.[126]

Probleme beim Fermat-Test

Im obigen Beispiel wurde bereits im zweiten Schritt herausgefunden, dass es sich bei *341* nicht um eine Primzahl handelt. Es gibt jedoch auch zusammengesetzte Zahlen, die den Test für sehr viele Basen *a* besteht. Da die Umkehrung des „kleinen Satzes von Fermat“ im Allgemeinen nicht gilt, ist es sogar so, dass zusammengesetzte Zahlen existieren, die den Fermat-Test für alle möglichen Basen *a* bestehen. Diese werden Carmichael-Zahlen[127] genannt. Solch eine Zahl wäre beispielsweise *561*. Obwohl es verhältnismäßig nur sehr wenige die-

[125] vgl. KARPFINGER & KIECHLE 2010, S. 144; OBLAK 2009, S. 30 f
[126] KARPFINGER & KIECHLE 2010, S. 144
[127] Benannt nach dem amerikanischen Mathematiker Robert Daniel Carmichael. Sie sind das Produkt von mindestens drei Primfakoren. Es existieren unendlich viele dieser Zahlen.

ser Zahlen gibt, bedeutet diese Tatsache, dass das Verfahren verfeinert werden muss, um es in der Praxis einsetzen zu können.[128]

Lucas-Test

Einer solchen Verschärfung bedient sich der Lucas-Test[129]. Hierbei wird eine zusätzliche Forderung eingeführt. Erfüllt eine Zahl den Fermat-Test, so muss weiters noch sichergestellt sein, dass kein echter Teiler m von $n-1$ die Bedingung

$$a^m \equiv 1 \bmod n$$

erfüllt. Ist dem so, handelt es sich bei der getesteten Zahl mit absoluter Sicherheit um eine Primzahl. Das Problem dieses Tests liegt auf der Hand. Dieses liegt in der Faktorisierung von $n - 1$ um alle echten Teiler zu erhalten. Allerdings lassen sich manche Zahlen mit einem besonderen Aufbau mittels Lucas-Test relativ einfach überprüfen, insbesondere Zahlen welche die Form $n = 2^k + 1$ besitzen, da hier alle echten Teiler von $n - 1$ Zweierpotenzen sind und daher einfach zu bestimmen sind. Dieser Test ist heutzutage in vielen erweiterten Formen im Einsatz, so zum Beispiel in Form des erweiterten Lucas-Test, des flexiblen Lucas-Test oder des Lucas-Lehmer-Test. Diese sollen hier jedoch nicht näher behandelt werden.[130]

Ein Beispiel zum Lucas-Test

Ein Beispiel soll diesen Test demonstrieren. Es soll mittels Lucas-Test überprüft werden, ob die Zahl $n = 59$ prim ist. Hierzu wird zunächst der Fermat-Test zur Basis $a = 2$ durchgeführt. Aus

$$2^{58} \equiv 1 \bmod 59$$

[128] vgl. PAAR & PELZL 2010, S. 189 f
[129] Benannt nach dem französischen Mathematiker Edouard Lucas, der den Test im 19. Jahrhundert vom Fermat-Test ableitete.
[130] vgl. MATTHES 2003, S. 184 f; OBLAK 2009, S. 31 f

folgt, dass es sich eventuell um eine Primzahl handeln kann. Nun wird $n - 1$ faktorisiert: $58 = 2 \cdot 29$. Für jeden dieser Primteiler, wird nun die zusätzliche Bedingung des Lucas-Tests durchgeführt:

$$2^2 \equiv 4 \bmod 59$$
$$2^{29} \equiv 58 \bmod 59$$

Da keiner dieser Primteiler die obige Bedingung erfüllt, handelt es sich bei 59 um eine Primzahl.

Rabin-Miller-Test

Der letzte Primzahltest, der hier noch behandelt werden soll ist der Rabin-Miller-Test[131]. Bei diesem handelt es sich um ein Testverfahren, das heutzutage sehr häufig zum Einsatz kommt. Dabei wird die zu testende Zahl in die Form

$$n = s \cdot 2^t + 1$$

mit natürliche Zahlen s und t gebracht, wobei t möglichst groß gewählt wird. Handelt es sich bei n um eine Primzahl, so ist zumindest eine der beiden folgenden Bedingungen erfüllt. Entweder gilt

$$a^s \equiv 1 \bmod n$$

oder

$$a^{s \cdot 2^r} \equiv -1 \bmod n$$

für ein $r \in \{0, \ldots, t - 1\}$. Der Nachweis dieser beiden Aussagen wird hier nicht durchgeführt, kann jedoch beispielsweise bei KARPFINGER & KIECHLE[132] nachgeschlagen werden. Diese beiden Bedingungen werden beim Rabin-Miller-Test überprüft. Sind beide nicht erfüllt, so handelt es sich bei n um eine zusammengesetzte Zahl. Andernfalls ist n möglicherweise eine Primzahl. Der Grund für

[131] Benannt ist dieser Test nach dem in Breslau (damaliges Deutsches Reich, heutiges Polen) geborenen Entwickler Michael Oser Rabin und dem amerikanischen Ideengeber Gary Lee Miller. Oftmals ist der Test auch unter Miller-Rabin-Test in der Literatur zu finden.
[132] KARPFINGER & KIECHLE 2010, S. 148

die häufige Anwendung dieses Verfahren liegt daran, dass die Irrtumswahrscheinlichkeit bei der Testung mit mehreren Zahlen *a* sehr rasch sinkt.[133]

Ein Beispiel zum Rabin-Miller-Test

Auch hier soll ein Beispiel das Testverfahren demonstrieren. Dazu soll die Zahl $n = 337$ mittels Rabin-Miller-Test überprüft werden. Dabei wird die Zahl im ersten Schritt in die benötigte Form gebracht:

$$n = 337 = 21 \cdot 2^4 + 1$$

In diesem Beispiel sind also die beiden Parameter $s = 21$ und $t = 4$. Anschließend wird ein zufälliger Wert $a = 120$ gewählt, mit dem getestet wird. Nun wird die erste Bedingung überprüft:

$$120^{21} \equiv 278 \bmod 337$$

Da das erhaltene Ergebnis nicht *1* lautet, kann noch keine Aussage getroffen werden. Aus diesem Grund wird nun die zweite Bedingung für alle $r \in \{0, \ldots, 3\}$ überprüft. Dabei kann gestoppt werden, wenn bei einer Überprüfung das Ergebnis *-1* lautet. In diesem Fall wäre die *337* wahrscheinlich prim. Entsteht dieses Ergebnis in keinem Testfall, so handelt es sich definitiv um eine zusammengesetzte Zahl. Die Überprüfungen liefern:

$r = 0: \quad 120^{21} \equiv 278 \bmod 337$

$r = 1: \quad 120^{42} \equiv 111 \bmod 337$

$r = 2: \quad 120^{84} \equiv 189 \bmod 337$

$r = 3: \quad 120^{168} \equiv -1 \bmod 337$

Da im letzten Überprüfungsschritt das Ergebnis *-1* lautet, ist die Zahl *337* wahrscheinlich eine Primzahl. Wird der Test nun mit weiteren Werten für *a* wiederholt, steigt die Wahrscheinlichkeit dafür, dass es sich um eine Primzahl handelt.

[133] vgl. SCHNEIER 2006, S. 304; WIESENBAUER 2012, S. 23

Der Test ist so effektiv, dass bereits nach *5* bestandenen Tests eine Wahrscheinlichkeit von über *99,9%* erreicht ist.[134]

[134] vgl. MATTHES 2003, S. 187

7 Bezug der Kryptographie zum Schulunterricht

7.1 Einleitung

Nachdem in den bisherigen Kapiteln die kryptologischen Themenbereiche eher von der fachlichen Sicht aus bearbeitet und betrachtet wurden, sollen in diesem Abschnitt die Einsatzmöglichkeiten im Schulunterricht beleuchtet werden. Diese sind vielfältiger als es auf den ersten Blick scheint. Dabei soll gleich klargestellt werden, dass im Folgenden keine Stundenbilder und Unterrichtsplanungen angeführt werden. Vielmehr sollen Möglichkeiten für den Einbau der Thematik, oder auch nur eines Teils davon, in den Schulunterricht aufgezeigt werden.

Berechtigung für den Einsatz – der Lehrplan

Die Grundlage für den Inhalt des Unterrichts in österreichischen Schulen bildet der Lehrplan. Die Lehrerin bzw. der Lehrer hat die Aufgabe, im Unterricht „entsprechend dem Lehrplan der betreffenden Schulart […] den Lehrstoff des Unterrichtsgegenstandes […] zu vermitteln“[135]. Aus diesem Grund soll zunächst geprüft werden, ob sich das Thema der Kryptologie im Schulunterricht diesbezüglich eignet.

Bereits im allgemeinen Teil des Lehrplans kann den allgemeinen didaktischen „Grundsätzen“ die Forderung nach der Einbindung und Bearbeitung „möglichst zeit- und lebensnahe[r] Themen“[136] entnommen werden, wobei den neuen und modernen Technologien verstärkte Bedeutung zukommen soll. Weiters wird im dritten Teil (Schul- und Unterrichtsplanung) festgehalten, dass ein Drittel der Unterrichtszeit, dem sogenannten Erweiterungsbereich zukommt. Dieser ist „durch die jeweilige Lehrerin bzw. den jeweiligen Lehrer […] zu planen“[137] und soll unter anderem nach Interessen und Begabungen der Schülerinnen und

[135] SchUG, §17 Abs 1
[136] BMUKK 2004d, Teil 2 Abs 7
[137] BMUKK 2004d, Teil 3 Abs 2

Schüler und des individuellen Schwerpunkts der Lehrerinnen und Lehrer zusammengestellt werden.[138]

Wird der Lehrplan für Mathematik der Oberstufe betrachtet, so können einige Dinge herausgelesen werden, die den Einsatz dieses Themas rechtfertigen. Zum einen befinden sich darin weitere allgemeine Forderungen, wie die Einbindung vielfältiger Aspekte sowie „mathematische[r] Beschreibung[en] von Strukturen und Prozessen der uns umgebenden Welt [und] die daraus resultierende vertiefende Einsicht in Zusammenhänge und das Lösen von Problemen durch mathematische Verfahren und Techniken“[139]. Weiters ist diesem zu entnehmen, dass der Unterricht vielfältige Anwendungsmöglichkeiten der Mathematik aufzeigen soll und diese auch in Form von fächerübergreifendem Unterricht bearbeiten soll.[140]

Ebenso können aus dem Bereich des Lehrstoffes Themen herausgelesen werden, die bei der Bearbeitung der Kryptologie Einsatz finden. Hierzu zählen unter anderem das Arbeiten mit Primzahlen und Teilern, das bereits in der Unterstufe behandelt wird, die Anwendung von Gleichungen in unterschiedlichen Bereichen und das Arbeiten mit Funktionen in der fünften Klasse und Berechnungen von Potenzen und das Arbeiten mit Vektoren in der sechsten Klasse.[141] Eine genaue Angabe, welche Lehrstoffbereiche bei welchem Teilgebiet der Kryptologie bearbeitet werden, ist in Abschnitt 7.3 zu finden.

Im Lehrplan für den Wahlpflicht-Unterricht in Mathematik befinden sich ebenfalls Passagen, die die Einbindung der Kryptologie ermöglichen. So heißt es bereits im ersten Satz, dass das Ziel dieses Unterrichts sein soll, „den Schülerinnen und Schülern gemäß ihrer Interessen eine Erweiterung bzw. Vertiefung ihres Bildungshorizontes zu bieten.“[142] Dabei werden keine Einschränkungen der behandelten Themenbereiche getroffen. Es wird jedoch der Einsatz des

[138] vgl. BMUKK 2004d
[139] BMUKK 2004a, S. 1
[140] vgl. BMUKK 2004a, S. 2
[141] vgl. BMUKK 2004a, S. 3 ff
[142] BMUKK 2004e

Computers als zentrales Element gefordert. Diese Forderung kann durch die Einbindung der Thematik Kryptologie durchaus erfüllt werden. In einer Auflistung möglicher Erweiterungsbereiche sind die Punkte Kryptologie und Codierung unter anderem ebenfalls angeführt.[143]

7.2 Einsatzgebiete im Unterricht

Die Einsatzmöglichkeiten der Kryptologie können in vielfältiger Form auftreten. Das Thema kann als klassischer Unterricht behandelt werden. Weiters bietet es eine gute Möglichkeit für Projektunterricht und fächerübergreifenden Unterricht. Hierbei können beispielsweise verschiedene Verfahren in Gruppenarbeit über einen längeren Zeitraum ausgearbeitet werden. Abschließend sollten die Ergebnisse den Mitschülerinnen und Mitschülern präsentiert werden. Dieser Unterricht kann auch in Kombination mit anderen Fächern erfolgen. Hierbei gibt es mehrere Möglichkeiten.

Fächerübergreifender Unterricht

Ein offensichtlicher Bezug besteht beispielsweise zur Informatik. Vor allem durch Programmierung und praktische Umsetzung diverser Algorithmen kann eine Verbindung hergestellt werden. Es können einfache Verschlüsselungsprogramme, beispielsweise das Cäsar-Verfahren oder die Vigenère-Verschlüsselung, von den Schülerinnen und Schülern selbst nachprogrammiert werden oder, im Falle von hoher Eigeninitiative, auch selbst entworfen werden. Mit solchen Aufgabenstellungen durfte ich um das Jahr 2000 selbst erste Programmiererfahrungen machen. Weiters können moderne Verfahren, wie RSA oder DES, ausgetestet und praktisch eingesetzt werden. Hierzu können diverse Programme, wie beispielsweise PGP[144] eingesetzt werden. Zusätzlich bilden auch die grundlegenden Inhalte der Zahlensysteme und des ASCII-Codes einen Bereich, der in der Informatik behandelt werden kann.

[143] vgl. BMUKK 2004e
[144] vgl. Anhang A

Zum Physikunterricht gibt es ebenfalls Verbindungsmöglichkeiten. Dies könnte durch die Behandlung der elektromechanischen Verschlüsselungsmaschinen geschehen. Hier können Teile aus physikalischer Sicht behandelt werden. Ebenso kann die Verbindung zur Quantenmechanik hergestellt werden. Da sich die Entwicklung quantenmechanischer Verfahren jedoch aktuell gerade erst in der Anfangsphase befindet, wurden diese hier nicht behandelt.

Für den fächerübergreifenden Unterricht eignet sich auch die politische Bildung. Vor allem der große Bereich des Datenschutzes eignet sich besonders gut. Hierbei kann einerseits die Notwendigkeit der Geheimhaltung von Daten besprochen werden, andererseits können damit auftauchende Probleme behandelt werden. Auch Gesetzte die die elektronische Kommunikation betreffen, bieten gute Verbindungsmöglichkeiten der Fächer Mathematik und politische Bildung.[145]

Wie Kapitel 4 (Geschichtliche Entwicklung der Kryptographie) zeigt, kann auch eine Verbindung zwischen Mathematik und Geschichte hergestellt werden. Dabei bietet sich einerseits die Entwicklung der ersten Verfahren an und andererseits kann die Entwicklung der Verschlüsselungsmaschinen und die dadurch entstehenden Auswirkungen auf den Verlauf des Zweiten Weltkriegs behandelt werden. Auch verschiedene andere geschichtliche Bereiche, wie beispielsweise Verschlüsselung während des Kalten Kriegs können bearbeitet werden. Ein Beispiel hierfür wäre das SALT2-Abkommen zwischen den USA und der Sowjetunion, bei dem es um geschaffene eine Obergrenze der Anzahl der nuklearen Langstreckenwaffen geht. Zur Überprüfung der Einhaltung dieser Grenze wurden kryptographische Verfahren eingesetzt, die sicherstellen mussten, dass die Anzahl an Waffen nicht überschritten wird. Gleichzeitig durfte allerdings die Position der Nuklearwaffen nicht verraten werden.[146]

Letztendlich bietet sich auch die Möglichkeit, eine der wenigen Verbindungen zwischen der Mathematik und dem Sprachunterricht herzustellen. Hier bieten

[145] vgl. STOHR 2007, S. 23
[146] vgl. SCHMEH 2007, S. 337 ff

die Buchstabenverteilungen und die Häufigkeitsanalysen bei der Kryptoanalyse von monoalphabetischen Verschlüsselungsverfahren eine Möglichkeit. Es gibt jedoch auch eine Verbindung zur Literatur. Es gibt eine Vielzahl von Werken, in denen die Behandlung von Kryptologie und Kodierung eine zentrale Rolle spielt. Diese können in einem fächerübergreifenden Unterricht ebenfalls sehr gut eingesetzt werden. Einige Beispiele hierfür wären:

- Brown, Dan – Diabolus

  Dieses Werk bietet einen Einblick in die Arbeiten rund um die Kryptologie. Es geht um den amerikanischen Geheimdienst, der sich mit der Entschlüsselung von Nachrichten beschäftigt. Hierbei wird die Verbindung zwischen der Verschlüsselung und dessen Sicherheit gebildet. Weiters wird der Staat als überwachendes Organ miteinbezogen.
- Brown, Dan – Illuminati, Sakrileg, Das verlorene Symbol

  In den drei Teilen einer Thriller-Reihe rund um einen amerikanischen Symbolologen geht es jeweils um einen anderen Mythos, dessen Existenz stets durch Verschlüsselung mit der Hilfe unterschiedlicher Symbole vertuscht wird. Im Lauf der Werke erhält der Leser einen Eindruck über die faszinierenden möglichen Bedeutungen unterschiedlicher Symbole.
- Burgess, Anthony – Clockwork Orange

  In diesem Roman nutzen die Hauptcharaktere eine geheime Sprache. Dabei sind die meisten Worte auf die russische Sprache zurückzuführen. Diese Geheimsprache kann als monoalphabetische Verschlüsselung interpretiert werden. Ein eigens angehängter Glossar ermöglicht das Lesen des Werks.
- Verne, Jules – Reise zum Mittelpunkt der Erde

  Die Vorlage zahlreicher Verfilmungen handelt von einer alten verschlüsselten Botschaft, die den Weg zum Erdmittelpunkt beschreibt. Diese Nachricht muss entschlüsselt werden, um das Abenteuer beginnen zu lassen.

Zahlreiche weitere Werke und Verfilmungen behandeln die unterschiedlichen Bereiche der Kryptologie und können für den fächerübergreifenden Unterricht genutzt werden.

Vorwissenschaftliche Arbeiten

Ein weiteres Anwendungsgebiet kann die Behandlung von Aufgabenstellungen im Zuge einer vorwissenschaftlichen Arbeit im Sinne der neuen Reifeprüfung sein. Es gibt einige Fragestellungen, denen interessierte Schülerinnen und Schüler nachgehen könnten. Da die Aufgabenstellungen der künftigen vorwissenschaftlichen Arbeiten in Form einer bearbeitbaren Frage oder Hypothese formuliert werden müssen[147], bieten sich unter anderem die folgenden Beispiele an:

- Wie beeinflusste der Einsatz der Verschlüsselungsmaschinen Enigma, Purple und SIGABA den Verlauf des zweiten Weltkriegs?
- Wie funktioniert das RSA-Verfahren und wo wird es eingesetzt?
- Wie kann die Häufigkeitsanalyse zur Kryptoanalyse von monoalphabetischen und polyalphabetischen Verschlüsselungen herangezogen werden?
- Wie kann das Problem des Schlüsselaustausches bei kryptographischen Verfahren gelöst werden?
- Wie können ausreichend große Primzahlen zur Schlüsselbildung bei modernen kryptographischen Verfahren gefunden werden?
- Wie wurde die Kryptologie zur Überprüfung der Einhaltung des SALT 2 Abkommens während des Kalten Kriegs eingesetzt?

Natürlich bildet die obige Liste nur einen sehr kleinen Auszug aus möglichen Aufgabenstellungen für vorwissenschaftliche Arbeiten.

[147] vgl. BMUKK 2011, S. 7

7.3 Einbau im Mathematikunterricht

Im Folgenden sollen die zuvor behandelten Teile der Kryptologie in kurzen Zügen auf den jeweiligen Lehrplanbezug beleuchtet werden. Dabei soll beschrieben werden, welche Bereiche der Mathematik jeweils bearbeitet werden können und wo sich diese im Lehrplan wiederspiegeln. Vorab soll erwähnt werden, dass die angegebenen Schulstufen auf eine AHS bezogen sind. Die Vorschläge können allerdings auch auf andere Schultypen umgelegt werden. Weiters soll erwähnt werden, dass die im Folgenden gegebenen zeitlichen Vorschläge nicht verallgemeinert werden können. Vielmehr handelt es sich um Angaben, die aufgrund unterschiedlicher Leistungs- und Wissensstände der Schülerinnen und Schüler abweichen können.

Monoalphabetische Verschlüsselung

Wie bereits in Kapitel 5.1 erwähnt wurde, bieten monoalphabetische Verschlüsselungsverfahren einen sehr guten Einstieg in die Thematik. Dies ist deshalb so, weil die Verfahren händisch gut durchführbar sind. Beispielsweise kann die Cäsar-Verschlüsselung einen solchen Einstieg bieten. Diese ist einerseits einfach durchzuführen und zeigt andererseits auch den historischen Bezug der Kryptographie sehr gut auf.

Das Cäsar-Verschlüsselungsverfahren kann mit Schülerinnen und Schülern bereits in der Unterstufe behandelt werden. Es handelt sich dabei um ein leicht vorstellbares Verfahren, das keine gröberen Schwierigkeiten mit sich bringen sollte. Auch die Kryptoanalyse mittels Häufigkeitsanalyse kann bereits in der Unterstufe behandelt werden. Im Lehrplan der 2. Klasse sind die Ermittlung von Häufigkeiten und das Arbeiten mit Prozenten angeführt. Speziell das Aufstellen von Häufigkeiten wird zum Knacken einer monoalphabetischen Verschlüsselung benötigt.[148]

[148] vgl. BMUKK 2004b

Transpositionsverschlüsselung

Der Einsatz von Transpositionsverschlüsselungen kann ebenso wie die Einbringung monoalphabetischer Verschlüsselungen bereits in der Unterstufe erfolgen. Hierbei können die Schülerinnen und Schüler einen spielerischen Zugang zur Thematik erhalten, der dazu dienen kann, Freude an der Thematik zu wecken. Beispielsweise könnte ein Papierstreifen um einen etwas dickeren Holzstab gewickelt werden. Auf diesen kann nun ein Text geschrieben werden, welcher durch Abwickeln verschlüsselt wird:

Abbildung 17: Transpositionsverschlüsselung im Unterricht[149]

Dieses Verfahren wurde bereits in Kapitel 5.3 (Transpositionsverschlüsselung) unter dem Namen Skytale vorgestellt. Soll von diesem Verfahren auf allgemeine geometrische Verschlüsselungsverfahren geschlossen werden, sollten die Schülerinnen und Schüler sich zumindest in der siebenten oder achten Schulstufe befinden, da zu diesem Zeitpunkt der Zusammenhang zwischen der spielerischen Variante und einem allgemeinen geometrischen Verschlüsselungsverfahren verstanden werden kann.[150]

Polyalphabetische Verschlüsselungsverfahren

Das Grundverständnis der Vigenère-Verschlüsselung sollte bereits bei Schülerinnen und Schülern der Unterstufe vorhanden sein. Dennoch sollte dieses Verfahren aufgrund seiner gegenüber monoalphabetischen Verschlüsselungsverfahren höheren Komplexität wohl eher erst gegen Ende der Unterstufe oder zu

[149] BORYS 2011, S. 261
[150] vgl. BORYS 2011, S. 261

Beginn der Oberstufe behandelt werden. BORYS[151] beschreibt als größtes Problem beim Umgang mit der Vigenère-Verschlüsselung im Schulunterricht, dass die Schülerinnen und Schüler beim „Heraussuchen des Ver- bzw. Entschlüsselungsbuchstabens verrutschen“. Das bedeutet, dass sie in der Tabelle die falsche Zeile oder Spalte erwischen und somit bei der Verschlüsselung oder bei der Entschlüsselung Fehler begehen, die ein korrektes Ergebnis nicht möglich machen.

Speziell die Kryptoanalyse des Vigenère-Verfahrens sollte nicht in einer Unterstufe durchgenommen werden. Es ist zwar nicht so, dass die genutzten Methoden und Verfahren sehr kompliziert sind. Allerdings handelt es sich um einen relativ umfangreichen Ablauf, der durchgeführt werden muss. Die Erarbeitung zur Kryptoanalyse könnte in drei Schritten erfolgen. Zunächst sollte den Schülerinnen und Schülern auf jeden Fall klargemacht werden, dass eine einfache Häufigkeitsanalyse nicht zielführend ist. Dies kann durch einfaches Probieren gezeigt werden. Im zweiten Schritt kann überlegt werden, wie ein verschlüsselter Text entschlüsselt wird, wenn die Länge des Schlüssels bekannt ist. Der letzte Schritt beinhaltet das Herausfinden der Schlüssellänge. Den Abschluss des Themas könnte ein Gesamtbeispiel, wie es in Kapitel 5.4 (Polyalphabetische Verschlüsselung) durchgeführt wurde, bilden.[152]

Die behandelten Themengebiete sind zum Einen die bereits bei der einfachen Häufigkeitsanalyse erwähnte Ermittlung von Häufigkeiten, zum Anderen kommt hier die Arbeit mit dem größten gemeinsamen Teiler dazu. Beide Themen sind im Lehrplan der 2. Klasse zu finden.[153]

DES

Da der DES ein computerbasierendes Verschlüsselungsverfahren ist, sollten die Schülerinnen und Schüler zur besseren Verständlichkeit bereits am Informatikunterricht teilgenommen haben, bevor das Verfahren behandelt wird. Aus

[151] BORYS 2011, S. 292
[152] vgl. STOHR 2007, S. 79 ff
[153] vgl. BMUKK 2004b

diesem Grund eignet sich die Behandlung des DES nicht in der Unterstufe. Die zu behandelnden Themen sind auch hier zu großen Teilen im Lehrplan verankert. Einerseits ist im Lehrplan der 5. Klasse[154] das „Darstellen von Zahlen […] in einem nichtdekadischen Zahlensystem“ gefordert, was durch die Behandlung des binären Zahlensystems behandelbar wäre. Weiters kann die Funktionsweise des DES als Anwendung von Funktionen und Rekursionen dargestellt werden. Beide Themengebiete sind im Lehrplan der 6. Klasse zu finden.

Diffie-Hellman

Der Schlüsselaustausch nach Diffie und Hellman ist wohl eine Thematik, die idealerweise im vertiefenden Wahlpflichtfach behandelt werden kann. Dies hat den Grund, dass das Rechnen mit linearen Kongruenzen erforderlich ist. Dieses wird jedoch laut Lehrplan des Mathematikunterrichts in der Schule nicht unterrichtet.[155] Ein sicherer Umgang mit der Modulo-Rechnung erfordert jedoch einiges an Übung, sodass diese Thematik im Regelunterricht vermutlich keinen Platz finden wird. Ein Blick in den Lehrplan für den Wahlpflichtunterricht in Mathematik zeigt, dass die Kongruenzen hier in der Auflistung möglicher Themenbereiche zu finden ist.[156] Ein weiteres Gebiet, das benötigt wird um den Schlüsselaustausch zu behandeln, ist das Potenzieren. Dies ist im Lehrplan der 6. Klasse zu finden, weshalb eine Behandlung des Themas keinen Sinn macht.

Wird auch die Frage nach der Sicherheit des Verfahrens behandelt und insbesondere warum die Probleme im Umgang mit dem diskreten Logarithmus entstehen, so ist empfehlenswert, die Thematik frühestens in der 7. Klasse aufzugreifen, da die Schülerinnen und Schüler in der 6. Klasse den Logarithmusbegriff erst kennenlernen und dieser noch nicht gefestigt ist. Der wichtigste Aspekt, der beachtete werden muss, ist, dass die Zahlen mit denen gearbeitet wird, gut gewählt werden. Sonst ergeben die Potenzrechnungen schnell sehr große, unüberschaubare Zahlen. In der folgenden Tabelle sind für den Schulunterricht passende Zahlenkombinationen (bei denen die Ergebnisse der Poten-

[154] BMUKK 2004a
[155] vgl. BMUKK 2004a; BMUKK 2004b
[156] vgl. BMUKK 2004e

zen unter einer Million liegen) angegeben. Da *a* und *b* beliebig getauscht werden können, werden hier die Zahlenpaare nur einmal angeführt:

p	x	(a, b)
11	7	(2, 4)
13	2	(3, 7), (4, 5)
	4	(2, 5)
	6, 7	(2, 3), (2, 4)
17	2	(3, 5), (3, 6), (3, 7)
	3	(2, 4), (2, 6)
	5	(2, 4)
	9, 10, 14	(2, 3)

Abbildung 18: Einfache Zahlenkombinationen für den Schulunterricht[157]

RSA

Beim RSA-Verfahren werden ebenfalls Potenzen und Kongruenzen benötigt. Aus diesem Grund ist es vermutlich sinnvoll, auch diese Thematik nicht vor der 7. Klasse zu behandeln. Auch hier ist der geeignete Platz eher im Wahlpflichtfach. Weiters kommt hier zur Schlüsselpaarermittlung das Arbeiten mit dem größten gemeinsamen Teiler hinzu. Dies lernen die Schülerinnen und Schüler zwar bereits in der 2. Klasse, allerdings ist für das RSA-Verfahren das Arbeiten mit dem erweiterten euklidischen Algorithmus besser geeignet, weil durch diesen gleich das Inverse bestimmt werden kann, welches Teil des zugehörigen zweiten Schlüssels ist. Die Behandlung dieses Algorithmus kommt im Lehrplan zwar nicht explizit vor, er kann jedoch im Wahlpflichtfach durchaus eingebaut werden. Ähnlich wie beim Schlüsselaustausch nach Diffie und Hellman gilt auch beim RSA-Verfahren im Schulunterricht, dass die gewählten Zahlen nicht zu groß sein dürfen.

[157] vgl. BORYS 2011, S. 296

AES

Der AES ist vermutlich eines der Verfahren, die im Schulunterricht nicht behandelt werden sollten. Die Gründe dafür wurden bereits im Kapitel 6.5 (Advanced Encryption Standard (AES)) erläutert. Es gibt bei diesem Verfahren Teile, die die Anforderungen des Themas im Schulunterricht vermutlich übersteigen würden. Aus diesem Grund ist es sinnvoller, diese Thematik nicht zu behandeln, sondern stattdessen die Aufmerksamkeit anderen Verfahren zu widmen.

Primzahltests

Der Umgang mit den unterschiedlichen Primzahltests erfordert viel Übung und Geschick im Umgang mit linearen Kongruenzen. Die benötigten mathematischen Gebiete sind dieselben, wie beim Schlüsselaustausch nach Diffie und Hellman – Kongruenzen und Potenzieren. Weiters sollte vor den Primzahltests bereits das ein oder andere moderne kryptographische Verfahren behandelt worden sein. Diese zeigen nämlich erst die Notwendigkeit solcher Tests auf.

8 Literaturverzeichnis

BEUTELSPACHER u.a. 2008: Beutelspacher, Albrecht; Neumann, Heike B.; Schwarzpaul,Thomas (2008): Kryptographie in Theorie und Praxis. Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld. Vieweg+Teubner Verlag

BEUTELSPACHER 2009: Beutelspacher, Albrecht (2009); Kryptologie. Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. Ohne alle Geheimniskrämerei aber nicht ohne hinterlistigen Schalk, dargestellt zum Nutzen und Ergötzen des allgemeinen Publikums. Vieweg+Teubner Verlag

BEUTELSPACHER u.a. 2010: Beutelspacher, Albrecht; Schwenk, Jörg; Wolfenstetter, Klaus-Dieter (2010): Moderne Verfahren der Kryptographie. Von RSA zu Zero-Knowledge. Vieweg+Teubner Verlag

BMUKK 2004a: Bundesministerium für Unterricht, Kunst und Kultur: Lehrplan AHS Oberstufe (2004): Mathematik. [Zugriff: 27.04.2012]
Online unter: http://www.bmukk.gv.at/medienpool/11859/lp_neu_ahs_07.pdf

BMUKK 2004b: Bundesministerium für Unterricht, Kunst und Kultur: Lehrplan AHS Unterstufe (2004): Mathematik. [Zugriff: 27.04.2012]
Online unter: http://www.bmukk.gv.at/medienpool/789/ahs14.pdf

BMUKK 2004c: Bundesministerium für Unterricht, Kunst und Kultur: Lehrplan AHS Oberstufe (2004): Informatik. [Zugriff: 27.04.2012]
Online unter: http://www.bmukk.gv.at/medienpool/11866/lp_neu_ahs_14.pdf

BMUKK 2004d: Bundesministerium für Unterricht, Kunst und Kultur: Lehrplan AHS Oberstufe (2004): Allgemeiner Teil. [Zugriff: 27.04.2012]
Online unter: http://www.bmukk.gv.at/medienpool/11668/11668.pdf

BMUKK 2004e: Bundesministerium für Unterricht, Kunst und Kultur: Lehrplan AHS Oberstufe (2004): Mathematik Wahlpflichtfach. [Zugriff: 27.04.2012]
Online unter: http://www.bmukk.gv.at/medienpool/11884/lp_neu_ahs_29.pdf

BMUKK 2011: Bundesministerium für Unterricht, Kunst und Kultur (2011): Vorwissenschaftliche Arbeit. Eine Handreichung. Standardisierte, Kompetenzorientierte Reifeprüfung an AHS. [Zugriff: 27.04.2012] Online unter:
http://www.bmukk.gv.at/medienpool/20130/reifepruefung_ahs_vwa.pdf

BORYS 2011: Borys, Thomas (2011): Codierung und Kryptologie. Facetten einer anwendungsorientierten Mathematik im Bildungsprozess. Vieweg+Teubner Verlag

BUCHMANN 2010: Buchmann, Johannes (2010): Einführung in die Kryptographie. Springer Verlag

CZAKLER 2007: Czakler, Katharina (2007): Zahlentheorie im Schulunterricht. Möglichkeiten und Grenzen. Diplomarbeit TU Wien

DORNINGER 2004: Dorninger, Dietmar (2004): Anwendungen der Mathematik (für LAK). Modelle – Verfahren – Beispiele. Skriptum zur Lehrveranstaltung „Anwendungen der Mathematik“, Technische Universität Wien, Institut für Diskrete Mathematik und Geometrie, SS 2011

ECKERT 2004: Eckert, Claudia (2004): IT-Sicherheit. Konzepte, Verfahren, Protokolle. Oldenbourg-Verlag

EISLER 2008: Eisler, Andreas (2008): Elliptische Kurven und ihre Bedeutung in der Kryptographie. Diplomarbeit TU Wien

ERTEL 2007: Ertel, Wolfgang (2007): Angewandte Kryptographie. Carl Hanser Verlag

FREIERMUTH u.a. 2010: Freiermuth, Karin; Hromkovič, Juraj; Keller, Lucia; Steffen Björn (2010): Einführung in die Kryptologie. Lehrbuch für Unterricht und Selbststudium. Vieweg+Teubner Verlag

GOLUCH 2011: Goluch, Sigrun (2011): The development of homomorphic cryptography. Diplomarbeit TU Wien

HASIBEDER 2010: Hasibeder, Johannes (2010): Kryptographie mittels elliptischer Kurven im Mathematikunterricht. Diplomarbeit TU Wien

JANOWICZ 2006: Janowicz, Krzysztof (2006): Sicherheit im Internet. O‘Reilly Verlag

KARPFINGER & KIECHLE 2010: Karpfinger, Christine; Kiechle, Hubert (2010): Kryptologie. Algebraische Methoden und Algorithmen. Vieweg+Teubner Verlag

KIPPENHAHN 2006: Kippenhahn, Rudolf (2006): Verschlüsselte Botschaften. Nikol-Verlag

KLEIN 2007: Klein, Andreas (2007): Visuelle Kryptographie. Springer-Verlag

KÜSTERS & WILKE 2011: Küsters, Ralf; Wilke, Thomas (2011): Moderne Kryptographie. Eine Einführung. Vieweg+Teubner Verlag

LUNDE 2009: Lunde, Paul (2009): Die Welt der Codes. Geheime Botschaften und ihre Entschlüsselung. National Geographic Deutschland

MATTHES 2003: Matthes, Roland (2003): Algebra, Kryptologie und Kodierungstheorie. Mathematische Methoden der Datensicherheit. Carl Hanser Verlag

OBLAK 2009: Oblak, Sonja (2009); Öffentliche Chiffrierverfahren für die Schule und in der Praxis. Diplomarbeit TU Wien

PAAR & PELZL 2010: Paar, Christof; Pelzl, Jan (2010): Understanding Cryptography. A Textbook for Students and Practitioners. Springer-Verlag

REMPE & WALDECKER 2009: Rempe, Lasse; Waldecker, Rebecca (2009): Primzahltests für Einsteiger. Zahlentheorie – Algorithmik – Kryptographie. Vieweg+Teubner Verlag

SCHMEH 2004: Schmeh, Klaus (2004): Die Welt der geheimen Zeichen. Die faszinierende Geschichte der Verschlüsselung. W3L-Verlag

SCHMEH 2007: Schmeh, Klaus (2007): Codeknacker gegen Codemacher. Die faszinierende Geschichte der Verschlüsselung. W3L-Verlag

SCHNEIER 2006: Schneier, Bruce (2006): Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C. Pearson Studium

SCHUG : Schulunterrichtsgesetz - SchUG

SCHWENK 2010: Schwenk, Jörg (2010): Sicherheit und Kryptographie im Internet. Von sicherer E-Mail bis zu IP-Verschlüsselung. Vieweg+Teubner Verlag

SONNENSCHEIN 2011: Sonnenschein, Roman (2011): Attacken auf Public-Key-Kryptosysteme und ihre Implementierung in Maple. Diplomarbeit TU Wien

SPITZ u.a. 2011: Spitz, Stephan; Pramateftakis, Michael; Swoboda, Joachim (2011): Kryptographie und IT-Sicherheit. Grundlagen und Anwendungen. Vieweg+Teubner Verlag

STOHR 2007: Stohr, Monike (2007): Unterricht in Kryptologie. Dissertation Univ. München

WÄTJEN 2008: Wätjen, Dietmar (2008): Kryptographie. Grundlagen, Algorithmen, Protokolle. Spektrum Akademischer Verlag

WIESENBAUER 2012: Wiesenbauer, Johann (2012): Zahlentheorie und Anwendungen. Unterlagen zur Vorlesung „AKDIS Zahlentheorie und Anwendungen“, Technische Universität Wien, Institut für Diskrete Mathematik und Geometrie, SS 2012. [Zugriff: 27.04.2012]

Online unter: http://www.algebra.tuwien.ac.at/institut/zthanw/index.html

WRIXON 2006: Wrixon, Fred (2006): Geheimsprachen. Codes, Chiffren und Kryptosysteme, von den Hieroglyphen zum Digitalzeitalter. Tandem-Verlag

9 Abbildungsverzeichnis

Anhang A – Internetquellen zur Demonstration im Unterricht

Auf den folgenden Seiten im Internet sind die alphabetisch geordneten Verfahren für praktische Versuche anschaulich dargestellt. Hiermit können die vorgestellten Ver- und Entschlüsselungsarten im Unterricht praktisch durchprobiert werden. Natürlich handelt es sich hierbei nicht um eine vollständige Liste der verfügbaren Quellen. Die aufgelisteten wurden jedoch allesamt durchgetestet und veranschaulichen meistens auch die Berechnungen, die hinter den Verfahren stecken.

ADVANCED ENCRYPTION STANDARD:

http://www.formaestudio.com/rijndaelinspector/archivos/Rijndael_Animation_v4_eng.swf

[Zugriff: 27.04.2012]

CÄSAR VERSCHLÜSSELUNG:

http://www.ivhp.de/files/caesar.htm

[Zugriff: 27.04.2012]

http://www.lucius-hartmann.ch/diverse/kryptographie/caesar.html

[Zugriff: 27.04.2012]

DATA ENCRYPTION STANDARD:

http://people.eku.edu/styere/Encrypt/JS-DES.html

[Zugriff: 27.04.2012]

http://www.matheprisma.de/Module/DES/index.htm

[Zugriff: 27.04.2012]

FERMAT-TEST:

http://www.am.hs-mannheim.de/KryptoLern/fermat.php

[Zugriff: 27.04.2012]

HÄUFIGKEITSANALYSE:

http://www.kas-bc.de/krypto/analyse.php

[Zugriff: 27.04.2012]

KASISKI TEST:

http://www.staff.uni-mainz.de/pommeren/Kryptologie/Klassisch/2_Polyalph/kasiski1.html

[Zugriff: 27.04.2012]

LUCAS TEST:

http://www.hbmeyer.de/eratosib.htm

[Zugriff: 27.04.2012]

PGP (DOWNLOADLINK):

http://www.pgpi.org/

[Zugriff: 27.04.2012]

RABIN-MILLER-TEST:

http://www.johannes-bauer.com/compsci/millerrabin/index.php?

[Zugriff: 27.04.2012]

http://www.am.hs-mannheim.de/KryptoLern/miller-rabin.php

[Zugriff: 27.04.2012]

RSA VERSCHLÜSSELUNG:

http://cisnet.baruch.cuny.edu/holowczak/classes/9444/rsademo/

[Zugriff: 27.04.2012]

http://www.hanewin.net/encrypt/rsa/rsa-test.htm

[Zugriff: 27.04.2012]

VIGENERE VERSCHLÜSSELUNG:

http://fbim.fh-regensburg.de/~saj39122/oop/unterlagen/projekte/vigenere/java.html
[Zugriff: 27.04.2012]

http://www.lucius-hartmann.ch/diverse/kryptographie/vigenere.html
[Zugriff: 27.04.2012]

http://einklich.net/etc/vigenere.htm
[Zugriff: 27.04.2012]

Anhang B – Beispielsammlung für den Unterricht

Im Folgenden sind einige Beispiele gesammelt, die für die Behandlung der vorab beschriebenen Themen im Unterricht genutzt werden können.

Cäsar:

Beispiel 1: [158]

Der folgende Text ist mit einer Verschiebechiffre verschlüsselt.

```
Lpulu nhuglu kbtwmlu, kburslu buk zapsslu Olyizaahn shun
dhy pjo bualy ilkybljrluk uplkypnly Dvsrlukljrl kbyjo lpul
lpnluabltspjo vlkl Shukzjohma nlypaalu, ipz pjo, hsz kpl
Zjohaalu klz Hilukz olyhizhurlu, khz zjodlytblapnl Ohbz
Bzoly cvy tpy splnlu zho.
```

(aus E.A. Poe: ,,Der Untergang des Hauses Usher")

Auflösung:

Einen ganzen dumpfen, dunklen und stillen Herbsttag lang war ich unter bedrueckend niedriger Wolkendecke durch eine eigentuemlich oede Landschaft geritten, bis ich, als die Schatten des Abends herabsanken, das schwermuetige Haus Usher vor mir liegen sah.

Beispiel 2: [159]

Und Cäsar sprach: `SBKF SFAF SFZF`.

Auflösung:

VENI VIDI VICI.

Beispiel 3: [160]

Der Schlüsseltext `JIVSOMPMQUVQA` wurde mit der Verschiebungschiffre erzeugt. Ermitteln Sie den Schlüssel und den Klartext.

Auflösung:

Schlüssel: 8

Klartext: BANKGEHEIMNIS

[158] BEUTELSPACHER u.a. 2008, S. 19
[159] BEUTELSPACHER 2009, S. 20
[160] BUCHMANN 2010, S. 92

Diffie-Hellman:

Beispiel 4: [161]

Führe das Kommunikationsprotokoll DIFFIE-HELLMAN mit den folgenden Werten durch:
$p = 13$, $x = 2$, $a = 5$ und $b = 7$.
Wie lautet am Ende der gemeinsame Schlüssel s?

Auflösung:

$A \equiv 2^5 \bmod 13$ → $A = 6$

$B \equiv 2^7 \bmod 13$ → $B = 11$

$B^a \equiv 11^5 \bmod 13$ → $s = 7$

$A^b \equiv 6^7 \bmod 13$ → $s = 7$

Euklidischer Algorithmus:

Beispiel 5: [162]

Berechne jeweils mit dem erweiterten Euklidischen Algorithmus den größten gemeinsamen Teiler von a und b und stelle diesen als ganzzahlige Linearkombination von a und b dar.
(a) $a = 22$, $b = 24$
(b) $a = 3$, $b = 10$
(c) $a = 100$, $b = 125$

Auflösung:

(a) ggT (22, 24) = 2
$2 = -1 \cdot 22 + 1 \cdot 24$
(b) ggT (3,10) = 1
$1 = -3 \cdot 3 + 1 \cdot 10$
(c) ggT (100,125) = 25
$25 = -1 \cdot 100 + 1 \cdot 125$

[161] FREIERMUTH u.a. 2010, S. 212
[162] FREIERMUTH u.a. 2010, S. 293

Häufigkeitsanalyse:

Beispiel 6: [163]

Der folgende Text ist monoalphabetisch verschlüsselt.

Ocs yif jcs Cvtirsfcv scvsf udscvsv bfivzesocoatsv Bifm, jcs Oatstsfszijs tcsoo, jio scvzcks Deuid cv jsf Msjcvi, jio yistfsvj jsf kivzsv Viatx ebbsv yif. So yif mivatmid kivz dssf, mivatmid oioosv jfsc ejsf pcsf Dsgxs jifcv. Ysvv so irsf pedd yif, im tisgbckoxsv zycoatsv zysc gvj jfsc Gtf viatxo, tesfxs miv lsjso Yefx, jio jcs ivjsfsv Kisoxs oikxsv, gvj uim mcx lsjsm cvo Ksonfisat.

(aus E. Canetti, ,,Die Stimmen von Marakesch")

Auflösung:

Sie war die Inhaberin einer kleinen franzoesischen Farm, die Scheherezade hiess, das einzige Lokal in der Medina, das waehrend der ganzen Nacht offen war. Es war manchmal ganz leer manchmal sassen drei oder vier Leute darin. Wenn es aber voll war, am haeufigsten zwischen zwei und drei Uhr Nachts, hoerte man jedes Wort das die anderen Gaeste sagten und kam mit jedem ins Gespraech.

Beispiel 7: [164]

Der folgende Kryptotext wurde mit CAESAR aus einem deutschen Text erzeugt, und zur besseren Lesbarkeit wurden die Buchstaben gruppiert, wobei die Gruppierung nichts mit der Länge der tatsachlichen Wörter zu tun hat.

IVVIP IBIVM QVMUI VLMZM VBIOO MJCZB ABIOI TAITM F.

Bestimme die absoluten Häufigkeiten der einzelnen Buchstaben und versuche durch das Bestimmen der häufigsten Buchstaben direkt auf den Schlüssel zu schließen.

Auflösung:

Schlüssel: 8

Klartext: Anna hat an einem anderen Tag Geburtstag als Alex.

[163] BEUTELSPACHER u.a. 2008, S. 19
[164] FREIERMUTH u.a. 2010, S. 98

Primzahltests:

Beispiel 8: [165]

Beweisen Sie mit dem Fermat-Test, dass 1111 keine Primzahl ist.

Auflösung:

$2^{1110} \equiv 1024 \bmod 1111$ → keine Primzahl

Beispiel 9: [166]

Führen Sie den Rabin-Miller-Test für die Eingabe n=25 aus. Gehen Sie dabei davon aus, dass das zufällig gewählte a den Wert 2 hat. Geben Sie die Werte an, die b der Reihe nach annimmt. Finden Sie ein $a \in \{2, \ldots, n-2\}$, für das der Miller-Rabin-Test (mit obigem n) eine falsche Ausgabe liefert.

Auflösung:

$n = 25 = 3 \cdot 2^3 + 1$ → s = 3, t = 3

r = 0: $2^3 \equiv 8 \bmod 25$

r = 1: $2^6 \equiv 14 \bmod 25$

r = 2: $2^{12} \equiv 21 \bmod 25$ → keine Primzahl

falsche Aussage für a = 7:

r = 0: $7^3 \equiv 18 \bmod 25$

r = 1: $7^6 \equiv -1 \bmod 25$ → möglicherweise prim

RSA:

Beispiel 10: [167]

Bestimme aus dem gegebenen öffentlichen Schlussel (*n, e*) von RSA und aus dem gelüfteten Geheimnis $\phi(n)$ die restlichen Teile *p*, *q* und *d* des privaten Schlüssels.

(a) $n = 11\,639$, $e = 4415$, $\phi(n) = 11\,424$

(b) $n = 28\,363$, $e = 22\,403$, $\phi(n) = 28\,000$

(c) $n = 201\,563$, $e = 112\,483$, $\phi(n) = 200\,640$

(d) $n = 64\,523$, $e = 10\,201$, $\phi(n) = 63\,840$

Auflösung:

(a) $p = 103$, $q = 113$, $d = 9887$

(b) $p = 251$, $q = 113$, $d = 13\,067$

(c) $p = 353$, $q = 571$, $d = 71\,947$

(d) $p = 571$, $q = 113$, $d = 54\,121$

[165] BUCHMANN 2010, S. 132
[166] KÜSTERS & WILKE 2011, S. 181
[167] FREIERMUTH u.a. 2010, S. 335

Beispiel 11: [168]

Verschlüsseln Sie mit dem RSA-Algorithmus bei p=23, q=59 und e=15 den Klartext M = 348 613 407 195 771 184. Warum wäre hier e=11 keine gute Wahl für den öffentlichen Schlüssel?

Auflösung:

C = 725 596 607 10 588 1081

e=11 ist keine gute Wahl, weil 11 Teiler von 1276 (=$\phi(n)$) ist. Deshalb ist die Inverse zu 11 modulo 1276 nicht eindeutig und der geheime Schlüssel kann nicht bestimmt werden.

Transposition:

Beispiel 12: [169]

Wie lautet der Klartext, der zu folgendem, mittels einer Skytala chiffrierten Geheimtext gehört?

I S A D T P I H E H N N C S D I R O O I L T A I H T A E A S
N F E Z C S W E S S N I S F I U K T U J S E S T C R C K E !

Auflösung:

Ich wusste ja dass diese Transpositionschiffre leicht zu knacken ist!

Vigenere:

Beispiel 13: [170]

Der folgende Text ist mit dem Vigenere-Verfahren chiffriert. Bestimmen Sie zunächst die Schlüssellänge und rekonstruieren Sie anschließend den Text!

Stt woyej lllkisef Tfmekc fatr ek gy. Mazeef oy dwx Yaune lskftwzp dsy Eedkqof jceasll, mto dak Dtasxe ss lnvkcef Kydw lcayzp nsis jwslnvkx, dwx pr fonhl clr. Nopl kvlelkc, ady pr at oej Rlgw elr, vgcuwhpr fgnh ra oefqpn, ogd maz the mpsunlh, kuwllk pr ra oee Ynhdads cuxmwt, yiunes aye waxvlais amydej jpm Raqadr. Lbwx oak clr nopl kvlelkc. Ae gyfstr wsxpn woyfsis nmx oak Kceamyik ayd kktnw Lzlyky.

(aus P. Auster: "Stadt aus Glas")

Auflösung:

Schlüssel: Glas

[168] ERTEL 2007, S. 97
[169] BEUTELSPACHER 2009, S. 19
[170] BEUTELSPACHER u.a. 2008, S. 20

Mit einer falschen Nummer fing es an. Mitten in der Nacht laeutete das Telefon dreimal, und die Stimme am anderen Ende fragte nach jemandem, der er nicht war. Viel spaeter, als er in der Lage war, darueber nach zu denkenm was mit ihm geschah, sollte er zu dem Schluss kommen, nichts ist wirklich ausser dem Zufall. Aber das war viel spaeter. Am Anfang waren einfach nur das Ereignis und seine Folgen.

Beispiel 14: [171]

Verschlüssle den Klartext `FELDSTECHER` mit VIGENERE und dem Schlüssel `GLAS`.

Auflösung:

`LPLVYEEUNPR`

Beispiel 15: [172]

Der folgende deutsche Text wurde mit VIGENERE und einem Schlüssel aus vier Buchstaben verschlüsselt. Dabei wurden die Leer- und Satzzeichen des Klartextes beibehalten.

```
VMOIUP UHUPRMDSECEPN MJNH XVCCB FTNCHP BYTZNXFCHYJEEH WZN
AFHOYIYLCDSEH TNHCGQEH. TTE MDSWCNXEH OTCBU YUL BY DYS
HAMTPRICPRZMLEWIP, SIOOELO DCBXPBYO TM QBDSYS. OIY ULU-
WIQABSE IMU OAM ILUJULNQFYDOORSAFMIYU. SIYS DOFMEE XJP
GYTLMNF XAMTP GYOLU AMPIWI OEL NLSMF OEM WPRXSLEHHEEH XLS-
MFCS MFTN. XJPSYS KUMULNX XTRX BWLYSOIHHD NCF REHBF ELSPI-
WIE. ECOPRMFTTM XTREFY SCDS NUFXLCDS SYMMSN LWECODTY
VYTYSDCBJPDY AHIMDSEH EPR OCZONNLSMF FNX EPR XFD VYSO-
RUFYGNFY WUTDELT LUM. BYDYSPRMFTTM WPRUFYDYSE SCDS DCF OI-
WIEE XFD UGHPBYOOEH XLSMFCS FBFFYOO DOSNH UFYDYSFNAFY DYT
DAFAREBBWTYT, OEL NPNAF GOH TNHQFMEMUZFZFY UHE OEL UP-
MJFCANVC DYT HAMTPRM. ELS OCZON ILT UMDO CNXEL FTNY HPR-
CORE NFYDYOK ZO TEECHPN IEPR TV DIHLPN OOO MOTD DUIPR
YJYGYTEEOFCT QFCDYO, HOTV HAMTPR CO OEH SPGYMKEFMPN
TVREZMFTYU ZDYS LUMHPDLVPCEU HILE.
```

(a) Wie lautet der Klartext?
(b) Welches Wort ist der Schlüssel?

[171] FREIERMUTH u.a. 2010, S. 141
[172] FREIERMUTH u.a. 2010, S. 142

Auflösung:

(a) UBoote unterscheiden sich durch einige Besonderheiten von gewoehnlichen Schiffen. Sie schwimmen nicht nur an der Wasseroberflaeche, sondern schweben im Wasser. Die Tauchfahrt ist das Hauptanwendungsgebiet. Hier sollte die gesamte Masse genau gleich der Masse des Vergraengten Wassers sein. Dieser Zustand wird allerdings nie genau erreicht. Einerseits wirken sich naemlich selbst kleinste Unterschiede zwischen der UBootmasse und der des verdraengten Wassers aus, andererseits veraendert sich die Dichte des umgebenden Wassers laufend durch Aenderungen des Salzgehaltes, der Menge von Schwebestoffen und der Temperatur des Wassers. Das UBoot hat also immer eine geringe Tendenz zu steigen oder zu sinken und muss daher eingesteuert werden, wozu Wasser in den Regelzellen zugeflutet oder rausgedrueckt wird.

(b) Blau

Beispiel 16: [173]

Entschlüsseln Sie den folgenden Vigenere-verschlüsselten Text. (Das Schlüsselwort hat die Lange 4.)

```
IIVV SIUR ZWKU QRAV ZHLN HSVM GYMO QVHR GKMA PEAF QWSR
URON ZDTR UGPG QWQF FIQA QQMG TSLR PIZT QLMV YWKU DMNG
LYNV ZHMA PMMQ QVMA FWKU XYMF EITH ZKBE AXHG
```

Auflösung:

Wenige Menschen sind davon zu ueberzeugen, dass es kein ganz leichtes ist eine Methode der Geheimschrift zu finden, die der Entschluesselung trotzt.

Beispiel 17: [174]

Der folgende Geheimtext wurde mit einer Vigenere-Verschlüsselung erzeugt. Wir vermuten, dass der Klartext mit komme beginnt.

```
WCZFE SAFTX NFGAI XRKUB OTRZQ BGKEL RDHGK Z
```

Wie lautet der Klartext?

Auflösung:

Schlüssel: MONTAG

Klartext: Komme morgen zum vereinbarten Treffpunkt.

[173] KLEIN 2007, S. 13

[174] KLEIN 2007, S. 13

Eigenhändig unterfertigte Erklärung

„Ich erkläre, dass ich die vorliegende Diplomarbeit selbst verfasst habe und dass ich dazu keine anderen als die angeführten Behelfe verwendet habe. Außerdem habe ich die Reinschrift der Diplomarbeit einer Korrektur unterzogen und ein Belegexemplar verwahrt.“

Mathias Buzek