

Ein Angebot von  heise online

Anmelden



mehr Infos



Stöbern



&gt; @ctmagazin &gt; Story &gt; Der Dialog der Schwestern

# Der Dialog der Schwestern



@CTMAGAZIN | STORY

Bild: Illustration: Michael Thiele, Dortmund

 [Carsten Elsner](#)  18.01.2019 [Code](#), [Dialog der Schwestern](#), [Mathematik](#), [Schwestern](#), [Zahlenrätsel](#)

**Zwei Schwestern in einer psychiatrischen Privatklinik schicken sich geheime Botschaften. Die fiktive Kurzgeschichte von Carsten Elsner aus c't 25/1999 erklärt anschaulich, wie asymmetrische Verschlüsselung funktioniert.**

Als Martin den Bus verlässt, hat er sein Ziel schon fast erreicht. Vor ihm, am Ende einer leicht ansteigenden Kastanienallee, steht das Haus, in dem er als Zivildienstleistender in den nächsten Monaten leben und arbeiten wird. Es ist eine psychiatrische Privatklinik, ein modernes, im Stil eines großen Landschlusses erbautes Sanatorium. Über der Mitte des Gebäudes ragt ein Turm auf; er wirkt von Martins Standpunkt aus wie ein riesiger Wächter am anderen Ende der Allee. Das wilde Odenwald-Gebirge ringsum unterstreicht nur die Unfreundlichkeit dieses Ortes.

In den ersten Tagen ist Martin damit beschäftigt, sich in seiner neuen Umgebung zurechtzufinden. Er muss sich nicht nur bei Vorgesetzten, Ärzten und beim Pflegepersonal vorstellen und sich mit den Gepflogenheiten in dem weitläufigen Gebäude vertraut machen, er hat sich vor allem auf die Allgegenwart der psychisch kranken Menschen einzustellen.

Hier leben Menschen, die aus nicht ganz unvermögenden Verhältnissen stammen und deren Angehörige ihnen den Aufenthalt in dieser vergoldeten Abgeschiedenheit finanzieren können. Martin fällt schon bald auf, dass sehr schwere Fälle psychischer Erkrankungen in diesem Haus nicht vorkommen, obwohl es von der Ausstattung her dafür geeignet wäre. In den meisten Fällen ist den Menschen ihre Abweichung von der Norm auf den ersten Blick nicht anzusehen; nur beim Sprechen oder durch ihre Verhaltensauffälligkeiten tritt ihre Andersartigkeit zu tage. Was Martin jedoch gleich recht ungewöhnlich erscheint, ist das Durchschnittsalter der Bewohner. Es dürfte kaum über 25 Jahren liegen.

Martin missfällt die fast klösterliche Personalführung: An der Spitze der Klinik stehen der Chefarzt, ein gewisser *Professor Goldmann*, und sein Bruder in der Funktion des Finanzberaters. Dann kommen die Ärzte, gefolgt von den hauptamtlichen Pflegern, und an letzter Stelle stehen die Zivis - das Schlusslicht ist Martin als der Neuling im Hause. Gehorsam ohne Gegenfragen wird groß geschrieben.

Er hält sich von seinen Kollegen fern und beschränkt Kontakte auf das Tagesgeschäft und einige freundliche Worte bei den Mahlzeiten. Gott sei Dank ist ihm zum Wohnen in diesem goldenen Käfig ein bescheidenes Einzelzimmerchen zugewiesen worden. Hierher zieht er sich abends gerne allein zurück, wenn von den Zivis nur noch Rufbereitschaft erwartet wird.

Nach einer Woche der Einarbeitung wird Martin von der Pflegeleitung sein zukünftiges Arbeitsfeld zugeteilt. Dies besteht aus drei nebeneinander liegenden Appartements, deren Bewohner unter seine besondere Pflege und Aufsicht gestellt werden. Von nun an, da Martin in näheren Kontakt zu *Rudolf, Anna, Bianca* und *Doris* tritt, beginnt er, seine Eindrücke aufzuschreiben.

Als ich mit *Dr. Weissenborn* bei Anna eintrat, stand sie sofort von ihrem Stuhl auf und begrüßte uns mit den Worten: »Die Toren sprechen in ihrem Herzen: ‚Es ist kein Gott.‘ Sie taugen nichts; ihr Freveln ist ein Gräuel; da ist keiner, der Gutes tut.« - Das stammte aus der Bibel, die aufgeschlagen vor Anna auf dem Tisch lag (nach Annas eigener Aussage: *Psalter*, 53, 2; ich habe das sogar nachgeprüft: es stimmt). Ihr Lebensinhalt besteht nach Dr. Weissenborn im Bibelstudium, wobei sie sich ausschließlich auf den Psalter beschränkt. Sie ist 22 Jahre alt, Autistin und stammt aus einem streng katholischen Elternhaus. Anna weiß sicher gar nicht, wie hübsch sie ist. Ihr Äußeres vernachlässigt sie aber völlig zu Gunsten ihres Bibelstudiums. Ihren Ehrgeiz richtet sie auf lange Bibelzitate, die sie auswendig aufsagt. Ob sie wohl

versteht, um was es in den Texten geht? Von mir nahm sie keine weitere Notiz, jedenfalls habe ich keine Reaktion aus ihren Gesichtszügen abgelesen, als Dr. Weissenborn sie auf mich aufmerksam gemacht hat. Beim Verlassen ihrer Wohnung hörten wir zum Abschied noch: »Gott, sei mir gnädig, denn Menschen stellen mir nach; täglich bekämpfen und bedrängen sie mich.« (*Psalter*, 56, 2)

Auch Rudolf hat autistische Züge. Als wir sein Zimmer betraten, stand er in der Mitte des Raumes und schwankte mit dem Oberkörper hin und her. Kaum hatte der Siebzehnjährige mich erblickt, sprang er auf mich zu, baute sich mit seinen eins neunzig vor mir auf und brüllte: »Spielst du Schach?!« Dabei schaute er mich aber nicht einmal an. Ich war erschrocken und stotterte verlegen: »Ich kenne wenigstens die Regeln.«

»Dann lass uns spielen!« Von irgendwoher hatte er plötzlich ein Taschenschachbrett in den Händen. »Du musst immer auf deinen Turm Acht geben, sonst hole ich mir den zuerst!« »Später, Rudolf, später«, beruhigte ihn Dr. Weissenborn. »Der Martin muss jetzt noch arbeiten.« »Aber er hat versprochen, mit mir zu spielen!« »Ja, Rudolf, aber nicht jetzt. Vielleicht heute Abend.« »Aber ...«

Mit Mühe rissen wir uns los. Draußen im Gang meinte Dr. Weissenborn zu meinem Erstaunen: »Lass dich bloß nicht auf ein Spiel mit Rudolf ein. Ehe du dich versiehst, bist du schachmatt. Er ist ein Schachmeister; woher er die Erfahrung hat, wissen wir nicht. Er kann nicht einen Buchstaben lesen, und wenn er dich anschreit, so nimms ihm nicht krumm. Er hat beim Sprechen keine Kontrolle über die Lautstärke. Und übrigens hat mich Rudolf eben noch an etwas erinnert, was du unbedingt wissen musst: Der Turm hier im Hause ist für dich tabu! Das ist der Privatbereich vom Chef und seinem Bruder. Deshalb ist vor dem Treppenaufgang hinten im Gang auch ein Gitter angebracht. Wenn es mal offen steht, lass dich bloß nicht verleiten, da hinaufzugehen. Das gibt Ärger, und nicht zu wenig.«

Weissenborn sprach diese Warnung ziemlich scharf aus, und ich war wieder mal eingeschüchtert, wie so oft schon, seit ich hier bin.

Weitere Fragen dazu konnte ich auch gar nicht stellen, denn aus Biancas und Doris' gemeinschaftlich bewohntem Zimmer drang uns ein seltsamer Lärm entgegen.

»Nun kommt erst der pure Wahnsinn«, sagte Weissenborn, und er sollte Recht behalten. Wir hörten das Lachen der Schwestern durch die Tür, und ich glaubte schon, mit denen kann es wohl lustig werden. Aber als wir eintraten, setzten die beiden Frauen unbeirrt ihre Unterhaltung fort: »Dreihundertfünfundachtzig, achttausendzweihundertsechundsiebzig ...« Mit zungenbrecherischer Geschwindigkeit warfen sie sich Zahlen zu, die für sie einen Sinn ergeben mussten, denn sie hörten sich dabei gegenseitig aufmerksam zu.

»Guten Morgen, Bianca, guten Morgen, Doris. Wie geht es euch? Ich möchte euch

Martin vorstellen. Er wird in der nächsten Zeit auch bei uns hier wohnen. Martin, das ist Bianca und das ihre Schwester Doris.«

Gekicher. Ein ‚Guten Morgen‘ bringen beide unter Gelächter hervor. Dann schienen sie sich in ihrer Zahlensprache köstlich über mich zu amüsieren. Später klärte mich Dr. Weissenborn auf: »Jeder hier glaubt, dass sie mit ihrem Zahlensalat nur schauspielern und uns allen ein Gespräch vorgaukeln. Anderenfalls wäre das ja wohl auch ein ganz ungewöhnliches Phänomen.«

Ich kann ihm nur beipflichten.

Es dauert gar nicht so lange, bis Martin das Vertrauen von Anna, Rudolf, Bianca und Doris gewonnen hat. Eine gewisse Routine stellt sich bald ein: Bei den Bibelsprüchen Annas muss man einfach weghören. Mit Rudolf hat Martin schon so manche Schachpartie versucht: Er ist immer der hoffnungslos Unterlegene. Wenn er dann seinen matt gesetzten König auf dem Brett umlegt, springt Rudolf auf, läuft durch das Zimmer und freut sich jedes Mal kindisch über seinen Sieg.

Bianca und Doris hat Martin besonders ins Herz geschlossen. Beide sind Ende dreißig und leben schon lange in dieser Klinik. Mit ihnen kann er sich auf normale Weise durchaus über manchen belanglosen Vorfall im Hause unterhalten. Sie sind immer gut gelaunt und meistens etwas albern. Nur, ein längeres Gespräch mit Bianca und Doris ist unmöglich. Schlagartig setzen die Schwestern ihren Dialog in Zahlenhieroglyphen fort, und Martin ist ausgeschlossen.

Eines wird ihm bald klar: Hinter den Zahlenkolonnen verbirgt sich kein Chaos, sondern eine Geheimsprache. Immer wenn Martin die Schwestern etwas Persönliches fragen möchte, etwa was sie beide von Dr. Weissenborn oder Professor Goldmann halten, verlassen sie sofort die Ebene der herkömmlichen Sprache. Martin spürt hierin auch den Grund ihrer fortwährenden Heiterkeit: Sie wissen, dass ihrem Dialog keiner folgen kann, und das verleiht ihnen absolute Sicherheit. Wahrscheinlich wissen sie über vieles im Sanatorium genau Bescheid, nur würden sie es einem Dritten in Worten nie mitteilen, zumal ihre Welt an den Türen der Klinik ihre Grenzen hat. Weil Martin die Schwestern mag, tut ihm das ein wenig weh. Er würde sich mit ihnen gerne über manches unterhalten, natürlich nur im Rahmen ihrer Ausdrucksmöglichkeiten - aber eben in der Umgangssprache, nicht in Zahlen.

Im Laufe der Zeit hat er sich an die Strenge gewöhnt, mit der die Zivis hier behandelt werden, aber sie bleibt für ihn dennoch grundlos. Im Stillen beobachtet Martin aufmerksam die Ärzte und Pfleger, und zunehmend beschleicht ihn ein eigenartiger Verdacht.

Professor Goldmann und seinen Bruder bekommt man nicht oft zu Gesicht. Sie verlassen ihre Räume im Turm nur selten; meistens wird Martin an ihre Existenz nur dann erinnert, wenn die beiden Brüder mit ihrem Porsche die Kastanienallee hinauf-

oder hinunterbrausen. Immer verlassen sie gemeinsam das Sanatorium und kehren ebenso dorthin zurück. Martin wird aus diesem Verhalten nicht schlau. Dennoch scheint Professor Goldmann ein besonderes Interesse an jedem Neuzugang in der Klinik zu haben. Er allein entscheidet über die Aufnahme oder die Zurückweisung eines Patienten, und dabei fühlt er sich nicht an die Begutachtung durch Ärzte und Psychologen gebunden. Martin hat einmal ungewollt ein Gespräch zwischen zwei Klinikärzten durch eine nicht ganz fest geschlossene Tür mitverfolgen können. Dabei hat er Einblick in die Gepflogenheiten bei der Aufnahme eines Patienten erhalten. Das bestärkte ihn in seinem Verdacht, dass in diesem Haus etwas Ungewöhnliches vorgeht.

An einem langen und dunklen Herbstabend hat Rudolf `seinen Zivi´ zum Schachspielen überredet. Da Martin nichts Besseres zu tun hat, beginnt er mit Rudolf eine Partie nach der anderen. Zwar verliert er jedes Spiel und gibt Rudolf so mehrfach Anlass zu hemmungsloser Freude, aber er schärft dabei seine analytischen Fähigkeiten und verbessert zusehends seine Spielstrategien. Er ist immer wieder erstaunt, was er von Rudolf alles beim Spiel lernen kann. Die Uhr zeigt schon eine Stunde nach Mitternacht, als Martin - im Gegensatz zu Rudolf - das dringende Bedürfnis nach seinem Bett verspürt. Auf dem Weg durch die langen Korridore zu seinem Zimmer hört er in dem stillen Haus plötzlich die Schritte von mehreren Personen in seiner Nähe. Instinktiv bleibt er auf der halbdunklen Treppe stehen und lässt die Leute unten im Gang vorübergehen. Er sieht, wie drei Pfleger zwei Patienten, einen jungen Mann und eine Frau, zu Professor Goldmann in den Turm bringen. Niemand bemerkt ihn auf dem Treppenabsatz, seine Müdigkeit ist schlagartig verflogen. Von diesem ungewöhnlichen Vorgang überrascht, schleicht Martin erst nach einiger Zeit in sein Zimmer und schließt mit weichen Knien die Tür hinter sich.

Einige Tage nach diesem Vorfall findet Martin beim Aufräumen von Biancas und Doris´ Appartement im Bad eine einzelne Karte aus einem Skatspiel. Sie ist halb verdeckt hinter den Spiegel geklemmt. Er wundert sich ein wenig und bringt die Karte ins Wohnzimmer, wo er sie zu den übrigen Karten in eine Schublade legen will, in der die Schwestern einige Gesellschaftsspiele aufbewahren.

Martin hat es längst aufgegeben, bei seinen Schutzbefohlenen nach einem Sinn jeder ihrer Handlungen zu fragen. Als er jedoch die wild in der Schublade verstreuten Skatkarten ordnen will, stutzt er: alle Karten sind auf der Rückseite mit Zahlen beschrieben. Sie sind stets in Paaren angeordnet, und jedes Zahlenpaar ist bis auf ein einziges auf jeder Karte mit einem Bleistift wieder ausgestrichen worden. Martin untersucht die Karte, die er eben im Bad gefunden hat. Das auf ihr nicht gelöschte Zahlenpaar lautet: 14857, 3.

Da dringt plötzlich das Gelächter der beiden Schwestern von draußen herein; sie kommen gerade vom Frühstück aus dem Gemeinschaftsraum in ihr Zimmer zurück. Martin stößt rasch die Schublade zu und lässt die Karte aus dem Bad in seiner

## Hosentasche verschwinden.



Bianca und Doris wechseln kurz ein paar Worte mit ihm, albern herum und verfallen dann wieder in ihre Geheimsprache. Der junge Mann überlegt, ob er es wagen soll: Er werkelt erst noch ein wenig im Zimmer herum, dann wendet er sich zum Gehen. Ehe er aber die Tür hinter sich schließt, ruft er laut und vernehmlich ins Zimmer zurück:

»Vierzehntausendachthundertsiebenundfünfzig, drei.«

Augenblicklich entfährt beiden Schwestern ein kurzer Schrei. Bianca stürmt ins Bad, kommt aber gleich wieder heraus und schaut Martin fragend an. Der hält ihr die gefundene Karte entgegen, die aber keine von beiden zurücknehmen will. Dann schließt er die Tür, sein Herz pocht bis zum Halse. Zum ersten Mal hat er die beiden Schwestern in Verlegenheit gesehen. Offensichtlich ist dieses Zahlenpaar 14857, 3 ein Schlüssel zum Verständnis ihrer Sprache.

Martin nimmt sich fest vor, dieses Rätsel zu lösen. Vielleicht, ja vielleicht kann er irgendwann an den Gesprächen der Schwestern teilnehmen. Wenn sie ihn dabei akzeptieren, erfährt er vielleicht mehr über dieses Sanatorium.

Martin ist so in Gedanken vertieft, dass er auf dem Gang beinahe mit Anna zusammenstößt. Völlig entrückt, ohne irgendetwas um sich herum wahrzunehmen, monologisiert sie: »Gott, hilf mir! Denn das Wasser geht mir bis an die Kehle. Ich versinke in tiefem Schlamm, wo kein Grund ist; ich bin in tiefe Wasser geraten, und die Flut will mich ersäufen. Ich habe mich müde geschrien, mein Hals ist heiser. Meine Augen sind trübe geworden, weil ich so lange harren muss auf meinen Gott!« (*Psalter* 69, 2-4)

Martin ist im Augenblick nicht bereit, sich mit Anna auseinander zu setzen. Er lässt sie stehen und geht weiter seinen Gedanken nach: »Diese ausgestrichenen Zahlenpaare auf den Karten - das müssen Tagescodes sein, auf die sich die Schwestern morgens im Bad einigen. Ja, natürlich, so wird es sein. Aber: Bianca und Doris werden mir sicher nichts erklären können; ich kann mich nur versuchsweise in ihre Dialoge einmischen, um herauszubekommen, ob ich auf dem richtigen Weg bin.«

Da das erste Problem schon damit anfängt, dass die Schwestern ihre Zahlen sehr schnell sprechen, besorgt sich Martin in der Mittagspause in der Klinikverwaltung ein ausrangiertes Diktiergerät. Er gibt vor, beim Lesen eines medizinischen Lehrbuches Notizen auf Band festhalten zu wollen, um sie später schriftlich auszuarbeiten. Die Sekretärin sieht ihn zwar scheel von der Seite an, aber sie rückt das Gerät schließlich heraus. Zurück in seinem Zimmer holt Martin die bei den Schwestern gefundene Spielkarte hervor und studiert die Zahlenpaare auf der Rückseite:



Auffallend ist, dass die erste Zahl eines Paares immer bedeutend größer ist als die zweite. Mangels eines besseren Einfalls geht Martin von der nahe liegenden Grundvoraussetzung aus, dass in einer Geheimsprache die 26 Buchstaben des Alphabets den ersten 26 Zahlen zugeordnet sind. Martin fertigt sich hierzu eine Tabelle an.

Aber so einfach ist es bei den Schwestern nicht: Sie operieren mit viel größeren Zahlen, und für diese einfache Tabelle benötigte man auch keinen Schlüssel in Form eines Zahlenpaares.

»Wenn dieser Ansatz richtig ist«, überlegt Martin, »so werden mit Hilfe des Zahlenpaares die Zahlen von 1 bis 26, die für die jeweiligen Buchstaben stehen, auf andere, größere Zahlen abgebildet, und zwar so, dass man das auch wieder eindeutig auf die Zahlen 1 bis 26 zurückrechnen kann; vorausgesetzt, man kennt den Schlüssel. Aber wie geht das hier, nach welchen Regeln?«

Martin ist frustriert: es gibt beliebig viele Möglichkeiten für eine solche Kodierung. »Hier muss ich anders vorgehen, einen Versuchsballon starten«, denkt er. Er holt einen Schreibblock hervor und denkt lange über einen kurzen Satz nach, in dem möglichst viele Buchstaben mehrfach vorkommen. Schließlich schreibt er in großen Lettern über das ganze Blatt:

**ICH BIN BIANCA**

»Und nun zum Schlüssel. Damit ich eine Chance habe, bei der Kodierung dieser Worte später eine Gesetzmäßigkeit zu entdecken, muss ich das Zahlenpaar möglichst

geschickt wählen. Die zweite Zahl des Paares nehmen die Schwestern immer recht klein; was geschieht wohl, wenn ich sie auf 1 setze? Dann könnte ihr Einfluss bei der Kodierung vielleicht erst einmal ziemlich gering sein.«

Martin ist mit dieser Arbeitshypothese zufrieden.

»Und wie wähle ich die erste Zahl des Schlüssels?«

Hierzu will Martin nichts Rechtes einfallen. Schließlich hält er es für das Einfachste, sie mit der Anzahl der Buchstaben des Alphabets gleichzusetzen. So notiert er noch in der linken oberen Ecke des Blattes: 26, 1

Martin blickt skeptisch auf das Ergebnis. »Hoffentlich bin ich nicht auf dem falschen Dampfer«, murmelt er vor sich hin. »Nun denn, mal schauen.«

Er klopft bei Bianca und Doris an die Tür.

»Herein.« Die Schwestern blicken Martin erwartungsvoll an; von der Unruhe, in die sie heute Morgen der Kartenfund versetzt hatte, ist nichts mehr zu spüren. Etwas verlegen tritt der Zivi an den Wohnzimmertisch heran, an dem die beiden Frauen sitzen. Mitten auf dem Tisch liegt eine Spielkarte; in großen Ziffern steht ein Zahlenpaar darauf. Die Schwestern machen keine Anstalten, die Karte vor Martin zu verbergen. Im Gegenteil: Da sie ihn immer noch stumm anblicken und jede seiner Bewegungen verfolgen, fühlt Martin sich eingeladen, in die Welt ihrer Geheimnisse einzutreten. Über diese stumme Aufforderung ist er unglaublich erleichtert, und er hat den Eindruck, sie sitzen hier schon lange am Tisch und haben auf ihn gewartet. Irgendwie fühlt er sich durch ihr Vertrauen sehr geehrt.

»Könnt ihr mir mal etwas übersetzen?« Er stellt das Diktiergerät auf den Tisch und schaltet es ein.

»Aber gerne doch«, erwidert Doris. Martin legt Bianca seinen vorbereiteten Bogen vor, weist auf die Codezahlen 26,1 und beobachtet die Gesichter der Frauen. Bianca lächelt, als ob ihr die geforderte Verschlüsselung viel zu einfach erscheint. Nach einigen wenigen Augenblicken sprudeln jedoch 12 Zahlen aus ihr hervor:

»139, 289, 112, 496, 1335, 612, 80, 2063, 365, 508, 133, 53.«

»Ein Glück, dass ich den Einfall mit dem Diktiergerät hatte«, denkt Martin bei Biancas Zungenschlag. Er nimmt das Gerät und den Bogen wieder an sich, fragt beiläufig, ob er für beide noch etwas tun könne, und verzieht sich rasch in sein Zimmer. Dort hört er das Diktiergerät ab und schreibt die Zahlen unter die Buchstaben:

I	C	H	B	I	N	B	I	A	N	C	A
139	289	112	496	1335	612	80	2063	365	508	133	53



Danach ist Martin ziemlich ratlos. »Der Buchstabe A ist also einmal mit 53 und einmal mit 365 chiffriert worden. Nach meiner Tabelle würde ich ihm aber die 1 zuordnen.«

Martin starrt auf das Papier. »Und irgendwie spielt die 26 als Verschlüsselungszahl dabei eine Rolle ...«  
Er führt mit der 26 die einfachste Rechenoperation, die Addition, aus, um von der 1 in die Nähe der 53 zu gelangen:

$$\begin{aligned} 1 + 26 &= 27 \\ 1 + 26 + 26 &= 53 \end{aligned}$$

»Ups. Ist das ein Zufall?« Wohl nicht, denn rasch rechnet Martin nach:

$$1 + 14 \cdot 26 = 365$$

»Da haben wir ja das Geheimnis: Jede Zahl kann den Buchstaben A repräsentieren, die bei der Division mit 26 den Rest 1 lässt. Also hätte Bianca für das A auch 79 wählen können, denn

$$1 + 3 \cdot 26 = 79$$

Und demnach kann ein Buchstabe durch ganz viele Zahlen repräsentiert werden. Raffiniert.

«Martin überprüft die übrigen Buchstaben aus Biancas Übersetzung:

$$\begin{array}{llll} \text{I} & \rightarrow & 9 & \rightarrow & 9 + 5 \cdot 26 = 139 \\ \text{C} & \rightarrow & 3 & \rightarrow & 3 + 11 \cdot 26 = 289 \\ \text{H} & \rightarrow & 8 & \rightarrow & 8 + 4 \cdot 26 = 112 \text{ usw.} \end{array}$$

»Das lässt sich auch wieder leicht zurückübersetzen. Man muss nur schauen, welchen Rest zwischen 1 und 26 eine Zahl bei der Division mit 26 lässt:

$$139 : 26 = 5 \text{ Rest } 9; \text{ also } 9 \rightarrow \text{I}$$

Martin lehnt sich zufrieden zurück. Einen ersten Zipfel des Geheimnisses hat er gelüftet. Doch welchen Einfluss hat nun dabei noch die zweite Zahl aus dem Schlüssel, die er bisher auf 1 gesetzt hatte? Martin radiert auf dem weißen Bogen die



Codezahlen 26,1 aus und fügt stattdessen 51, 3 ein; die 51 hat er willkürlich gewählt, mit der 3 verwendet er absichtlich noch eine besonders kleine Zahl.

Nach dem Abendessen sucht er die Schwestern wieder auf und lässt sich den Text mit dem neuen Schlüssel noch einmal chiffrieren. Jetzt liefert ihm Bianca, wieder unter Zuhilfenahme des Diktiergerätes:

I C H B I N B I A N C A

1647 741 665 1487 780 2897 620 525 2500 2336 486 1174

Da die erste Codezahl 51 ist, mutmaßt Martin aufgrund seiner bisherigen Erfahrung, dass es hier nur auf Reste bei der Division mit 51 ankommt; und so müssten Zahlen, die *denselben Buchstaben* chiffrieren, *denselben Rest* bei der Division mit 51 ergeben. Martin überprüft diese These zuerst und ermittelt mit einem Taschenrechner die Reste:

$$\begin{aligned} \mathbf{I:} \quad 1647 &= 32 \cdot 51 + \mathbf{15} \\ 780 &= 15 \cdot 51 + \mathbf{15} \\ 525 &= 10 \cdot 51 + \mathbf{15} \end{aligned}$$

$$\begin{aligned} \mathbf{C:} \quad 741 &= 14 \cdot 51 + \mathbf{27} \\ 486 &= 9 \cdot 51 + \mathbf{27} \end{aligned}$$

$$\mathbf{H:} \quad 665 = 13 \cdot 51 + \mathbf{2}$$

$$\begin{aligned} \mathbf{B:} \quad 1487 &= 29 \cdot 51 + \mathbf{8} \\ 620 &= 12 \cdot 51 + \mathbf{8} \end{aligned}$$

$$\begin{aligned} \mathbf{N:} \quad 2897 &= 56 \cdot 51 + \mathbf{41} \\ 2336 &= 45 \cdot 51 + \mathbf{41} \end{aligned}$$

$$\begin{aligned} \mathbf{A:} \quad 2500 &= 49 \cdot 51 + \mathbf{1} \\ 1174 &= 23 \cdot 51 + \mathbf{1} \end{aligned}$$

Die Darstellung eines Buchstaben mit demselben Rest bei der Division mit 51 hat sich somit bestätigt. Nun bleibt noch die Frage nach dem Einfluss der zweiten Codeziffer 3. Bis auf den Buchstaben **A** entsprechen die oben ermittelten Reste aber nicht mehr der natürlichen Nummerierung der Buchstaben des Alphabets mit den Zahlen 1 bis 26; ja,

bei **C** und **N** kommen mit 27 und 41 sogar Zahlen oberhalb von 26 vor. Das muss die Einwirkung der Codeziffer 3 sein. Bei der Division mit 51 können sich insgesamt 51 mögliche Reste ergeben, und irgendwie trifft die 3 hieraus eine Auswahl von 26 Stück und ordnet diesen Resten die Buchstaben des Alphabets zu. Martin springt vom Tisch auf und läuft wie ein Tiger im Käfig in seinem engen Zimmerchen auf und ab.

»Ich muss herausfinden, wie die 3 die Zahlen 1, 2 bis 26 verändert. Sonst komme ich nicht weiter«, redet er laut mit sich selbst. »Die einfachsten Rechenoperationen haben schon einmal zum Ziel geführt. Mal schauen«.

*Addition mit 3:*

**A** -> 1 ->  $1 + 3 = 4$   
**B** -> 2 ->  $2 + 3 = 5$

»Quatsch mit Soße! In Biancas Verschlüsselung kommt bei **A** wieder 1 und bei **B** die 8 heraus. Das hier wäre auch zu simpel.

*Multiplikation mit 3:*

**A** -> 1 ->  $3 \cdot 1 = 3$   
**B** -> 2 ->  $3 \cdot 2 = 6$

»Ist es auch nicht«, Martin stehen Schweißperlen auf der Stirn. Er schließt die Augen und sieht sich in seinem Mathe-Kurs in der Schule sitzen. »Bei *Dr. Bruckner* haben wir doch so viel gelernt. Ich war doch nicht der Schlechteste. Mir haben doch selbst die Formeln für Potenzen und Logarithmen keine Schwierigkeiten bereitet, im Gegensatz zu meinem Freund *Carsten* ...

Moment!«Martin spricht wieder laut mit sich selbst. »Potenzen ... die fortgesetzte Multiplikation!« Er stürzt an den Tisch und rechnet:

<b>A</b>	->	1	->	$1^3$	=	$1 \cdot 1 \cdot 1$	=	<b>1</b>
<b>B</b>	->	2	->	$2^3$	=	$2 \cdot 2 \cdot 2$	=	<b>8</b>
<b>C</b>	->	3	->	$3^3$	=	$3 \cdot 3 \cdot 3$	=	<b>27</b>
<b>H</b>	->	8	->	$8^3$	=	$8 \cdot 8 \cdot 8$	=	512 = 10 · 51 + <b>2</b>
<b>I</b>	->	9	->	$9^3$	=	$9 \cdot 9 \cdot 9$	=	729 = 14 · 51 + <b>15</b>
<b>N</b>	->	14	->	$14^3$	=	$14 \cdot 14 \cdot 14$	=	2744 = 53 · 51 + <b>41</b>

»Wou! Ich habs. Die zweite Zahl 3 im Code ist ein *Verschlüsselungsexponent*.« Martin springt vor Freude auf sein Bett. »Ich habe Bianca und Doris durchschaut. Jetzt gibts keine Geheimnisse mehr für mich.«

Martin kehrt an den Tisch zurück und verschlüsselt im Rausch seiner Freude das Wort **DANKE** mit dem Schlüssel **51, 3**:

<b>D</b>	->	4	->	4 <sup>3</sup>	=	64	=	51 + <b>13</b>	->	9 · 51 + <b>13</b>	=	<b>472</b>
<b>A</b>	->	1	->	1 <sup>3</sup>	=	1	=	<b>1</b>	->	21 · 51 + <b>1</b>	=	<b>1072</b>
<b>N</b>	->	14	->	14 <sup>3</sup>	=	2744	=	53 · 51 + <b>41</b>	->	2 · 51 + <b>41</b>	=	<b>143</b>
<b>K</b>	->	11	->	11 <sup>3</sup>	=	1331	=	26 · 51 + <b>5</b>	->	17 · 51 + <b>5</b>	=	<b>872</b>
<b>E</b>	->	5	->	5 <sup>3</sup>	=	125	=	2 · 51 + <b>23</b>	->	7 · 51 + <b>23</b>	=	<b>380</b>

Die Faktoren 9, 21, 2, 17 und 7 bei 51 hat Martin dabei willkürlich gewählt. Er schreibt das Ergebnis auf einen kleinen Zettel:

**51,3:** 472, 1072, 143, 872, 380

Im Laufschrift spurtet er durch die Gänge des Sanatoriums und steht nach wenigen Augenblicken vor Biancas und Doris' Zimmer. Er klopft an und schiebt den Zettel unter der Tür durch. Man hört, wie sich drinnen jemand der Tür nähert. Martin wartet und horcht angespannt. Ein von Bianca laut gesprochenes »Bitte sehr« gibt ihm die Bestätigung für die Korrektheit seiner Überlegungen und Rechnungen. Während er mit langsamen Schritten in sein Zimmer zurückkehrt, hört er im Weggehen noch das Gekicher der beiden Schwestern.

In den folgenden Tagen sieht man Martin nur missgelaunt und übernächtigt bei seiner Arbeit. Die anfängliche Euphorie über die Entdeckung des Verschlüsselungsmechanismus ist einer ziemlichen Frustration gewichen. Zwar hat er auf seinem Laptop ein Programm geschrieben, mit dem er nach Eingabe eines Codezahlenpaares alle Buchstaben verschlüsseln kann, aber die Dechiffrierung bereitet ihm heftiges Kopfzerbrechen. Selbst bei Kenntnis eines Schlüssels hat er keinen Plan, wie er aus der Zahl, die einen Buchstaben repräsentiert, die entsprechende Nummer zwischen 1 und 26 gewinnen kann, mit der er den Buchstaben im Alphabet identifizieren kann. Er beherrscht bisher nur die Technik der *Verschlüsselung*, aber nicht die der *Entschlüsselung*; und für eine Kommunikation mit Bianca und Doris ist gerade die Dechiffrierung besonders wichtig. Lediglich in dem Fall, wenn der Verschlüsselungsexponent auf 1 gesetzt wird, behalten die Buchstaben ihre alphabetisch vorgegebene Nummerierung von 1 bis 26, und eine einfache Division mit Rest führt dann von den Zahlen zu den Buchstaben zurück. Aber den Verschlüsselungsexponenten 1 benutzen die Schwestern nie ...

Wer weiß schon, nach welchem Schema Bianca und Doris ihre Worte in Zahlen verwandeln und wieder entschlüsseln? Selbst wenn dieser Mechanismus durch Formeln beschrieben werden kann und im Computer in einer gängigen Programmiersprache laufen sollte, heißt das noch lange nicht, dass Bianca und Doris nach denselben Prinzipien vorgehen. Schon die Geschwindigkeit, mit der sie dabei

ohne technische Hilfsmittel auskommen, ist ein Hinweis darauf, dass in ihren Köpfen wohl einiges *völlig anders* abläuft als bei anderen Leuten. Wie soll man sonst auch verstehen, dass *Mozart* eine zufällig irgendwo gehörte Messe später aus der Erinnerung fehlerfrei und komplett in Partitur niederschreiben konnte? Überhaupt waren Leute wie *Mozart* und *Einstein* Menschen, die nur das Glück hatten, dass sie mit den Resultaten ihrer ungewöhnlichen Vernetzung im Kopf höchste gesellschaftliche Anerkennung fanden. Zwischen Rudolfs scharfsinnigen Schachstrategien und der Fähigkeit Mozarts, eine ganze Oper nur im Kopf komponieren zu können, besteht kein gradueller Unterschied. Nur die Objekte sind andere und die Einstellungen der ‚normalen‘ Menschen zu ihnen. Wenn Anna den ganzen Psalter auswendig aufsagt, gehört sie in diesem Sinne zu den Gratwanderern zwischen Genie und Wahnsinn, auch wenn ihre Monologe niemand hören will.



In diesem Sanatorium geht etwas Unheimliches vor: Ich *spüre* es, und Bianca und Doris *wissen*, was es ist. Vielleicht werde ich noch einmal dahinter kommen. Wie kann Dr. Weissenborn die Schwestern nur für wahnsinnig halten? In einer von ihnen als feindlich empfundenen Umgebung vermittelt ihnen ihre verschlüsselte Kommunikation das Gefühl von Sicherheit. Ist es bei uns so genannten ‚Normalen‘ in der Welt draußen denn anders? Wer fürchtet nicht beim Homebanking oder am Geldautomaten den Zugriff Fremder auf seine kleinen Geheimnisse? Ohne Geheimnummern kommt heutzutage doch kein moderner Mensch mehr aus. Verrücktheit ist pure Definitionssache.

Trotz intensiven Nachdenkens scheitert Martin am Problem der Dechiffrierung von Biancas und Doris' Geheimsprache. Aber er gibt trotzdem nicht auf. Er nutzt einen freien Tag, fährt nach Heidelberg und trifft sich dort mit *Dr. Praetorius* im mathematischen Institut der Universität. Martin hatte sich mit diesem Herrn, dessen Namen er im Personenverzeichnis der Hochschule ausfindig gemacht hatte, telefonisch in Verbindung gesetzt und diesen Termin vereinbart. Der akademische Rat empfängt ihn freundlich und hört geduldig zu, als Martin ihm von seiner Arbeit, den Schwestern und ihrer Zahlensprache erzählt. Auch Dr. Praetorius ist von den Fähigkeiten der beiden Frauen fasziniert, hat aber auch keine Erklärung für dieses eigenartige Phänomen. Martin setzt ihm dann die Verschlüsselungstechnik auseinander, soweit er sie bereits analysieren konnte. Sein eigentliches Ziel, von den Schwestern etwas über gewisse Vorkommnisse im Sanatorium erfahren zu wollen,

erwähnt der Zivi dabei natürlich nicht.

»Haben Sie eine solche Karte mit den Verschlüsselungscodes mitgebracht?«, fragt Dr. Praetorius. Martin reicht ihm die Spielkarte, die er im Bad der Schwestern hinter dem Spiegel gefunden hatte, und der Rat tippt einige Zahlen aus den Verschlüsselungscodes in seinen Computer ein. Er lässt die Maschine rechnen, nickt zufrieden und wendet sich wieder Martin zu. »Sie wissen doch, was Primzahlen sind?« Martin ist um die Antwort nicht verlegen, solche Dinge hat er in der Schule bei Dr. Bruckner gelernt. »Das sind Zahlen ohne Teiler«, erwidert er. »Richtig, genauer gesagt, ohne *echte* Teiler, denn *jede* Zahl ist immer durch 1 und sich selbst teilbar. Die ersten Primzahlen sind:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29 ...

Ist Ihnen schon aufgefallen, dass die erste Zahl eines jeden Codepaares stets aus *zwei* Primzahlen zusammengesetzt ist?«

Martin schüttelt den Kopf.

»Schauen Sie, hier!« Der Rat weist auf den Bildschirm des Computers:

4267 = 17 · 251  
17819 = 103 · 173

»Die Zahlen 17, 251, 103 und 173 sind alle Primzahlen. Und gerade diese Primfaktorzerlegung der jeweils ersten Codezahl muss man kennen, um dechiffrieren zu können.

Sie fragten mich eben nach der Möglichkeit der Entschlüsselung. Ich will sie Ihnen erklären. In der Kryptografie, der mathematischen Teildisziplin, in der man Verschlüsselungstechniken untersucht und entwickelt, kennt man das Verfahren Ihrer beiden Schwestern aus dem Heim schon lange; es ist ein einfacheres Verfahren. Erschrecken Sie nicht. Es ist trotzdem sehr wirkungsvoll.

Das Geheimnis bei der Entschlüsselung beruht auf einer Erkenntnis, die wir dem alten *Fermat*\* verdanken. Und so geht es.«

Dr. Praetorius greift zu den Aufzeichnungen, die ihm Martin mitgebracht hat. »Sie haben den Satz ICH BIN BIANCA mit dem Schlüssel **51, 3** kodieren lassen, und beispielsweise für den Buchstaben **H** von Bianca die Zahl 665 erhalten. Die erste Zahl aus dem Schlüssel, die 51, wollen wir den *Hauptmodul* nennen, die 3 haben Sie als *Verschlüsselungsexponent* bezeichnet; das soll mir recht sein. Sicher wird es Sie jetzt überraschen, dass man einen *Entschlüsselungsexponenten* bestimmen kann. Und genau hierfür benötigen Sie die Primfaktorzerlegung des Hauptmoduls. Er ist hier 51. Sie haben die 51 damals willkürlich gewählt, und zufällig ist das auch ein Produkt von



zwei Primzahlen.«

Dr. Praetorius schreibt auf ein Blatt:

$$51 = 3 \cdot 17$$

»Jetzt verringern Sie die beiden Primfaktoren jeweils um 1 und multiplizieren die Resultate miteinander. Was dabei herauskommt, wollen wir den *Nebenmodul* nennen.«

$$\text{Nebenmodul} = (3 - 1) \cdot (17 - 1) = 2 \cdot 16 = 32$$

»Können Sie mir nun eine Zahl angeben, die folgende Eigenschaft hat: Wenn man sie mit dem Verschlüsselungsexponenten 3 multipliziert und anschließend das Produkt durch den Nebenmodul 32 teilt, bleibt bei dieser Division mit 32 der Rest 1 übrig?«

Martin überlegt kurz, dann hat er das Resultat: »Elf.«

»Sehr gut«, lobt ihn der Rat und schreibt:

$$(11 \cdot 3) / 32 = 1 \text{ Rest } 1, \text{ oder } 11 \cdot 3 = 33 =$$

»Woher kommt diese Eins, die bei der Division mit dem Nebenmodul als Rest übrig bleiben soll?«, fragt Martin.

»Egal, mit welchen Zahlen Sie auch hantieren, an dieser Stelle muss bei der Division mit dem Nebenmodul *immer* der Rest 1 übrig bleiben. Das hat mit der Erkenntnis des alten Fermat zu tun, die dieser Rechnung zu Grunde liegt. Ja, und die Zahl 11, die Sie eben ermittelt haben, ist der gesuchte Entschlüsselungsexponent.«

Martin staunt. »Soll ich jetzt die 665, die mir Bianca für den Buchstaben **H** genannt hat, elfmal mit sich selbst multiplizieren?« fragt er ungläubig.

»Sie machen dabei nichts falsch. Aber diese Zahl wird ziemlich groß. Da wir anschließend das Ergebnis wieder durch den *Hauptmodul* 51 teilen und dabei den Rest bestimmen wollen, bietet es sich an, von der Verschlüsselungszahl 665 bereits vor dem Potenzieren mit 11 den Rest bei der Division durch den Hauptmodul 51 zu ermitteln. Sie haben das in Ihren Aufzeichnungen ja schon getan.«

$$665 = 13 \cdot 51 + 2$$

»Anstelle der 665 dürfen Sie auch die 2 potenzieren. Das ist viel bequemer.«

$$2^{11} = 2048 = 40 \cdot 51 + 8$$

Martin staunt: Die 8 steht in seiner Tabelle für den Buchstaben **H**. »Und durch dieses Potenzieren mit 11 können Sie die ganze von Bianca genannte Zahlenkolonne wieder in die Buchstaben zurückverwandeln. Übrigens: Dieses Kodierungsverfahren lässt sich auch für Ihren Laptop leicht programmieren.«

»Darauf soll erst mal einer kommen«, meint Martin, »kein Wunder, dass ich diese Nuss nicht geknackt habe.«

Dr. Praetorius hat aber noch einen weiteren Trumpf in der Hinterhand: »In der Praxis können zwei Personen, die nach diesem Verfahren geheime Nachrichten austauschen, den Codeschlüssel - also den Hauptmodul samt Verschlüsselungsexponent - sogar *öffentlich* bekannt geben, vorausgesetzt, der Hauptmodul ist sehr, sehr groß.«

Der junge Mann sieht den akademischen Rat ungläubig an. Der aber lächelt und fährt fort: »Das Problem bei Kodierungen sind weniger die Verfahren. Die sind vielen bekannt und beruhen meist auf recht elementaren mathematischen Prinzipien. Die Kunst der Dechiffrierung besteht nämlich zumeist in der Zerlegung sehr großer Zahlen in ein Produkt von Primzahlen, wie wir es hier bei unserem Hauptmodul  $51 = 3 \cdot 17$  auch getan haben. Bei so kleinen Zahlen, auch solchen, wie sie Bianca und Doris verwenden, ist das kein Problem. Mit Tabellen oder mit der Hilfe eines Taschenrechners findet man die Zerlegung rasch. Aber stellen Sie sich ein dreihundertstelliges Hauptmodul vor, dessen beide Primfaktoren etwa hundertfünfzigstellig sind. Diese Primfaktoren bleiben natürlich geheim. Auch mit größeren Computern dauert es dann schon seine Zeit, bis ein Dritter diese Primfaktoren gefunden hat.«

Als Martin wieder den Bus besteigt, der ihn zurückbringt, brummt ihm der Schädel. Aber er ist nun voller Zuversicht, mit Bianca und Doris künftig unbegrenzt kommunizieren zu können. Mit Hilfe des Diktiergerätes, dem Laptop und seinem Wissen sollte das nun doch möglich sein. - Auf den Einfall, hundertstellige Codeschlüssel zu verwenden, wird er die Schwestern aber nicht bringen.

Obwohl Martin an diesem Abend erst spät in das Sanatorium zurückkehrt, entwirft er noch ein Entschlüsselungsprogramm. Schon auf der Busfahrt hatte er sich dazu einige Skizzen nach dem Dechiffrierungskonzept von Dr. Praetorius angefertigt. Er überprüft es mit dem Schlüssel **51, 3** an der Kodierung des Satzes ICH BIN BIANCA. Es läuft einwandfrei. Zusammen mit dem Verschlüsselungsprogramm, das er bereits vor einigen Tagen fertig gestellt hatte, verfügt Martin nun über ein komplettes Dolmetschersystem für die Geheimsprache der Schwestern. Dr. Praetorius hatte richtig vorausgesagt, dass die zugehörigen Programme gar nicht so kompliziert sind



und die Routinen sehr schnell laufen. Einzelne Wörter oder kurze Sätze kann man auch mit einem Taschenrechner bewältigen, aber keine längeren Gespräche. Hier hilft nur der Laptop. Übermüdet, aber mit sich selbst zufrieden, fällt Martin schließlich ins Bett.

Zu Martins ersten morgendlichen Pflichten gehört es, nach ‚seinen Leuten‘ zu sehen. Rudolf und Anna sind Langschläfer, aber Bianca und Doris stehen mit den Hühnern auf. Mit Herzklopfen betritt Martin ihr Zimmer; Diktiergerät und Laptop hat er schon bei sich. Die Schwestern sitzen schweigend an ihrem Wohnzimmertisch, auf Martins freundliches »Guten Morgen« reagieren sie nicht. Sie bleiben auch stumm, als er die beiden Geräte auf den Tisch stellt.

Sie müssen geahnt haben, dass er heute auf ihre Weise mit ihnen kommunizieren wird und absichtlich für Martin eine Spielkarte hinter dem Badezimmerspiegel verborgen. Die Losung des Tages lautet: 681, 151.

Martin setzt sich zu den Frauen an den Tisch. Er gibt den Codeschlüssel ein und übersetzt die Worte

Guten Morgen

Die Zahlen auf seinem Bildschirm liest er laut vor. Der Bann ist gebrochen. Die Schwestern antworten verschlüsselt, Martin übersetzt zurück. Anfangs benutzt er noch das Diktiergerät, aber schließlich merkt er, dass es auch ohne das Aufnahmegerät geht. Bald hat er Übung und tippt die Zahlen der Frauen direkt während ihrer Rede ein; sein Laptop übersetzt in Windeseile. Zwar geht es ein wenig langsamer voran, als es die Schwestern unter sich gewöhnt sind, weil Martin die Tastatur bedienen muss. Aber die Konversation ist flüssig.

Allmählich leitet Martin das Gespräch von den Belanglosigkeiten auf die Ärzte und Pfleger im Hause über. Schließlich ist es so weit: Er tippt mit zittrigen Händen die Frage

Was machen sie mit euch im Turm?

Während er die Zahlen der Chiffrierung vorliest, bekommt er einen trockenen Hals. Es ist Doris, die antwortet:

172, 1734, 315, 641, 372, 3491, 360, 387, 586, 602, 2358

»Eine kurze Antwort«, denkt Martin, ehe er die Taste zur Ausführung der Übersetzung betätigt. Es dauert keine Sekunde, bis das Gerät die Aufgabe bewältigt hat. Martin starrt fassungslos auf den Bildschirm seines Laptop. Er kann erst nicht glauben, was er liest. Aber dann handelt er rasch.

Wenige Tage später wird ein ungeheurer Skandal in der Odenwald-Klinik aufgedeckt und landesweit mit Empörung zur Kenntnis genommen.

\* *Pierre de Fermat, französischer Mathematiker, 1601 bis 1665*

*Anmerkungen des Verfassers: Um den Leser nicht zu verwirren, wurde bei der Beschreibung des Verschlüsselungsverfahrens eine notwendige mathematische Voraussetzung nicht erwähnt. Sie ist für den Verlauf der Geschichte auch nicht erforderlich. Nicht jedes beliebige Zahlenpaar ist als Verschlüsselungscode tauglich, wo der Hauptmodul ein Produkt von zwei Primzahlen ist. Vielmehr sollte darauf geachtet werden, dass der Hilfsmodul und der Verschlüsselungsexponent keinen gemeinsamen Teiler haben. Anderenfalls würde man keinen Entschlüsselungsexponenten finden. Beispiel: Das Paar 35,15 taugt nicht als Verschlüsselungscode, weil der Hilfsmodul  $(5 - 1) \cdot (7 - 1) = 24$  und der Verschlüsselungsexponent 15 den gemeinsamen Teiler 3 haben.*

*In praktischen Anwendungen des in der Geschichte beschriebenen so genannten RSA-Verfahrens (benannt nach seinen Erfindern Rivest, Shamir und Adleman) verschlüsselt man allerdings einen Text nicht buchstabenweise. Ist nämlich der Hauptmodul öffentlich bekannt, so kann man einen chiffrierten Text auf die Häufigkeit gewisser Reste hin statistisch untersuchen und kann so eventuell bei längeren Texten einzelne Buchstaben dechiffrieren, da man weiß, mit welcher Häufigkeit etwa in deutschen Texten die Buchstaben a oder e vorkommen. Man verschlüsselt daher einen Text blockweise, indem man die Buchstaben des Textes fortlaufend zu Blöcken fester Länge zusammenfasst und diesen Blöcken nach einem bestimmten Verfahren jeweils eine einzelne Zahl zuordnet.*

*Des Weiteren ist es - im Gegensatz zu Doris' und Biancas Vorgehensweise - in der Praxis üblich, die Verschlüsselung nicht in Form von Zahlenfolgen, sondern wieder in Buchstabenfolgen anzugeben, die als Text natürlich keinen Sinn ergeben. Details zu diesem RSA-Verfahren findet man in folgendem Buch:*

*Neal Koblitz: A Course in Number Theory and Cryptography, second edition, Kapitel IV, Paragraph 2; Springer-Verlag 1994.*

["Der Dialog der Schwestern" aus c't 25/1999 \(PDF\)](#)



<https://heise.de/-4274601>

[Drucken](#)

## KOMMENTARE

---



boxenbausatz // 19.01.2019 10:36

**Lösung bitte!**

Kann das bitte wer entschlüsseln, ich gestehe ich bin zu faul dazu!

[Antworten](#) [Zitieren](#) [E-Mail](#)

---



schneidergarak // 19.01.2019 17:53

**Re: Lösung bitte!**

So schwer ist das nun auch wieder nicht. Selbst als python-Einsteiger habe ich dafür nur eine halbe Stunde gebraucht.

Und aus der Geschichte lässt sich auch so ableiten was da passiert.

[Antworten](#) [Zitieren](#) [E-Mail](#)

---



Mirko Dölle // 19.01.2019 21:52

**Re: Lösung bitte!**

schneidergarak schrieb am 19.01.2019 17:53:

Und aus der Geschichte lässt sich auch so ableiten was da passiert.

Aber mit der exakten Lösung erscheinen Annas Zitate in einem gänzlich neuen Licht. Das macht die Geschichte so besonders.

Viele Grüße,  
Mirko Dölle

[Antworten](#) [Zitieren](#) [E-Mail](#)

---



fassi63 // 20.01.2019 00:17

**Re: Lösung bitte!**

... und Ende 1999 gab es ja einen aktuellen Bezug zur Odenwald- ... nein, nicht Klinik...

Excel hat übrigens auch ausgereicht.  
Danke für die Herausforderung!

[Antworten](#) [Zitieren](#) [E-Mail](#)

---



Mimmikri // 26.01.2019 15:41

**Re: Lösung bitte!**

schneidergarak schrieb am 19.01.2019 17:53:

Und aus der Geschichte lässt sich auch so ableiten was da passiert.

Ich hatte, nur ausgehend von der Wortlänge, zuerst was anderes vermutet.

Mirko Dölle schrieb am 19.01.2019 21:52:

Aber mit der exakten Lösung erscheinen Annas Zitate in einem gänzlich neuen Licht. Das macht die Geschichte so besonders.

Nicht nur die Zitate, auch Teile der Erzählung erscheinen in einem etwas anderen Licht.

[Antworten](#) [Zitieren](#) [E-Mail](#)



Dr. Peter Rottengatter // 20.01.2019 21:17

**Re: Lösung bitte!**

schneidergarak schrieb am 19.01.2019 17:53:

Selbst als python-Einsteiger habe ich dafür nur eine halbe Stunde gebraucht.

Manchmal ist eben auch das Schreiben eines Programmes einfach nur Overhead. In diesem Fall gelingt die Entschlüsselung mit einem nicht-programmierbaren Taschenrechner in etwa 10 Minuten.

[Antworten](#) [Zitieren](#) [E-Mail](#)



thoq // 23.01.2019 12:02

**Bitte sehr!**

Habe meinen Code bei repl.it (online-IDE) eingestellt:

<https://repl.it/repls/SnappyComfortableWifi>

Ich hoffe der Link ist permanent. Keine Ahnung, ob und wann die das löschen.

*Das Posting wurde vom Benutzer editiert (23.01.2019 12:16).*

[Antworten](#) [Zitieren](#) [E-Mail](#)



drphuebert // 23.01.2019 12:46

**Re: Bitte sehr!**

Ob das @boxenbausatz und @GrusGrus (u.v.a.) hilft, die Porno-Lösung zu finden?

[Antworten](#) [Zitieren](#) [E-Mail](#)



thoq // 23.01.2019 12:54

**Re: Bitte sehr!**

Wenn sie sich trauen, das Programm zu starten, dann schon...

[Antworten](#) [Zitieren](#) [E-Mail](#)



CREON, Christian Krause // 30.01.2019 01:02

**Re: Bitte sehr!**

Die Nachricht aus der aktuellen Geschichte kann ich damit aber leider nicht entschlüsseln.

Damit gibts eine Exception:  
TypeError: must be str, not int

[Antworten](#) [Zitieren](#) [E-Mail](#)



thoq // 30.01.2019 09:48

**Re: Bitte sehr!**

ja, im aktuellen Artikel wird eine etwas aufwendigere Verschlüsselung (in Blöcken) genutzt. Habe den Artikel bisher nur kurz überfliegen können. Arbeit geht halt vor 🙄

[Antworten](#) [Zitieren](#) [E-Mail](#)



thoq // 21.01.2019 18:45

**4757, 167**

69494 75389 96656 53858 53843 30547 \_ 47452 85627 92388  
18170 \_ 69371 30058 21644 66743 \_ 37333 35304 35177 91899  
61986 96656 78885 50343 23786 63846 49448 58600 33444 \_  
71356 38201 25663 65875 27684 63357 82400

[Antworten](#) [Zitieren](#) [E-Mail](#)

---



drphuebert // 22.01.2019 21:46

**Re: 4757, 167**

genau genommen, sind es zwei "sehr interessante Artikel", oder?

[Antworten](#) [Zitieren](#) [E-Mail](#)

---



thoq // 23.01.2019 11:31

**Re: 4757, 167**

Ja, absolut richtig. Den zweiten Artikel hatte ich zu dem Zeitpunkt aber noch nicht gelesen.

[Antworten](#) [Zitieren](#) [E-Mail](#)

---



drphuebert // 23.01.2019 12:41

**Re: 4757, 167**

Hm. Den Artikel von vor zwanzig Jahren hab ich halt erst als zweiten gelesen. Aber beziehend auf den aktuellen wäre ja zusätzlich eine verschlüsselte Signatur adäquat gewesen. Nicht, dass da jemand nachträglich heimlich den Text auf die Mehrzahlform ändert...

[Antworten](#) [Zitieren](#) [E-Mail](#)

---



GrusGrus // 22.01.2019 09:20

**Schade**

Als "Nichtprogrammier" und einer der mit Mathematik schon immer auf Kriegsfuss stand, ist es nach vielen Jahren als Leser das erste Mal, dass ich hier im Abseits stehe. Schade 🙄

[Antworten](#) [Zitieren](#) [E-Mail](#)



drphuebert // 22.01.2019 16:54

### Quersumme

Es steht doch "lediglich" zur Prüfung an, dass im aktuellen Heft 3/19 die Quersumme 128 richtig ist. Also dann starte mal, Kranich!

@Fassi63:

| **Excel hat übrigens auch ausgereicht.**

Eine Berechnung mit " $^{126197}$ " macht mein Excel nicht mit. 🤔

Aber auf wolframalpha.com per copy/paste rechnen zu lassen ist ja noch viiiieeel einfacher. Und die Rechenvorlagen sind doch ganz easy in der ZIP-Datei 🙄

[Antworten](#) [Zitieren](#) [E-Mail](#)



Mimmikri // 26.01.2019 15:54

### signed integer overflow

Zum [Schnell-Link](#) der aktuellen c't zu dieser Geschichte (Danke dafür!) gibt es kein Forum, daher hier: Das C-Programm zur Entschlüsselung kann, wegen des kleinen Exponenten, zwar die finale Nachricht entschlüsseln, bei den "Lernversuchen" am Anfang scheitert es aber:

```
$ gcc -fsanitize=undefined dialog-Programm.c
$ ./a.out 51 3

[...]

1647
dialog-Programm.c:35:18: runtime error: signed integer c
```

Die offensichtliche Lösung ist es, der Funktion

```
potenz
```

auch den Hauptmodul zu übergeben und nach jeder Multiplikation noch eine Modulo-Operation einzufügen. So bleiben die Zahlen ausreichend klein.

Das Posting wurde vom Benutzer editiert (26.01.2019 15:56).

[Antworten](#) [Zitieren](#) [E-Mail](#)

## Kommentar verfassen

Überschrift (bitte unbedingt ausfüllen)

**B**

*i*

u

✂

code

„Zitat“

Link

😊

Zitat trennen

### Stöbern

Suchbegriff

Q

Test & Kaufberatung

Praxis & Tipps

Wissen

Trends & News

@ctmagazin



[Bildmotive](#)

[c't-Projekte](#)

[Blog](#)

[Service](#)

[Jahresarchiv](#)

[Archiv vor 2012](#)

[RSS-Feed](#)

[Werben auf c't](#)

[Datenschutz](#)

[Impressum](#)



---

[Datenschutzhinweis](#) [Impressum](#) [Kontakt](#) [Mediadaten](#) 2578672

Content Management by **InterRed**

Copyright © 2019 Heise Medien