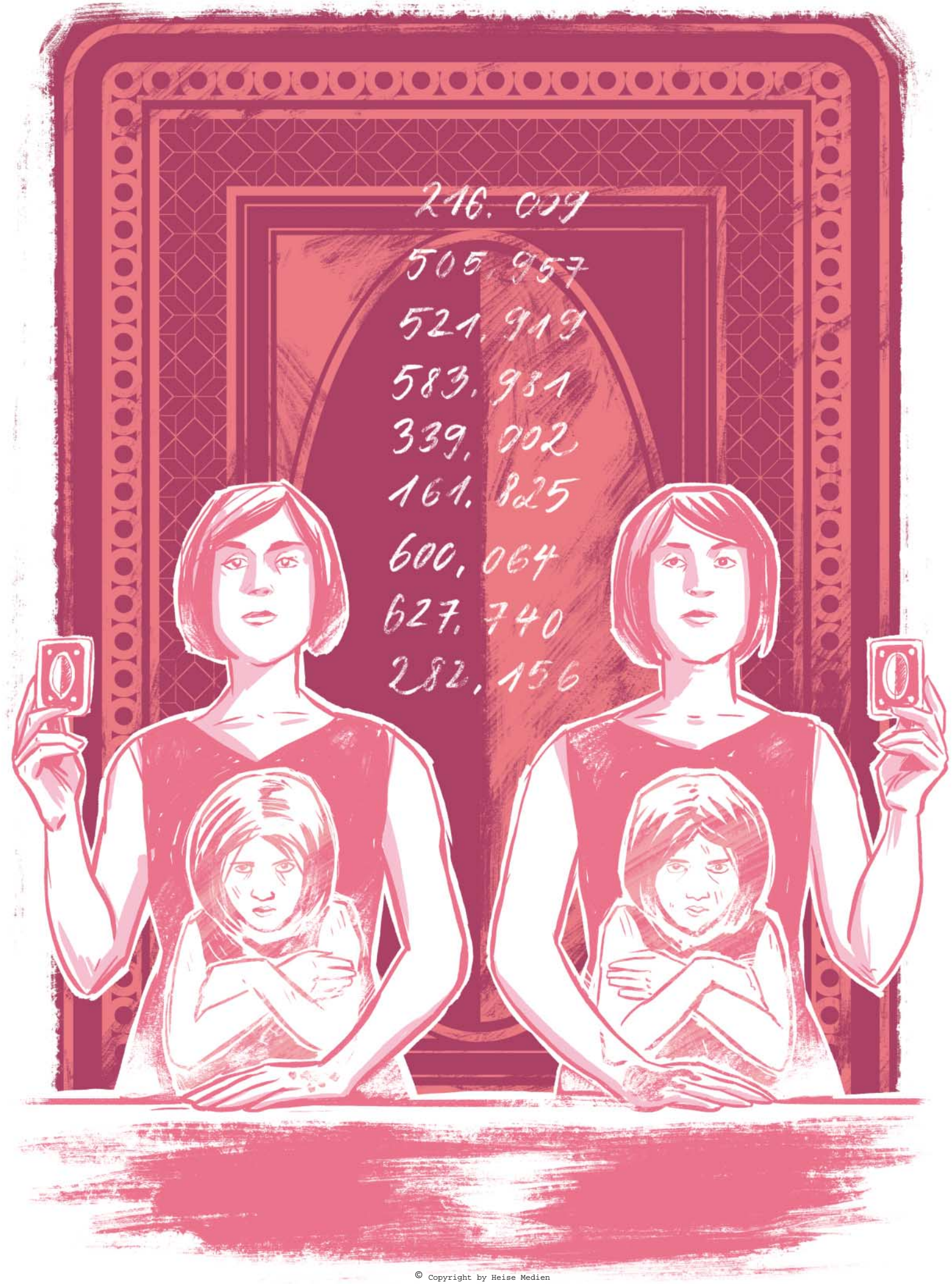

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

NEUES VON DEN SCHWESTERN

VON CARSTEN ELSNER

Wie ein Bühnenvorhang zerreißt die Schwärze, als Doris wieder zu sich kommt. Das Licht ist schmerzhaft hell, selbst durch ihre geschlossenen Lider hindurch. Deshalb dreht sie den Kopf zur Seite, bevor sie vorsichtig ihre Augen öffnet. Doch wo ist sie? Das ist nicht ihr Schlafzimmer. Sie kennt den muffigen gekachelten Raum nicht, von dessen Decke die blendende Lampe herabhängt. Aber sie erkennt die beiden Männer, die sichtlich zufrieden neben der harten Pritsche stehen, auf der sie liegt: Es sind Professor Goldmann, der ehemalige Chefarzt der Odenwaldklinik, und sein nicht minder krimineller Bruder.

Unwillkürlich versucht Doris, von den Männern wegzurücken. Doch sie kann sich nicht bewegen – sie ist an Armen, Beinen und Hüfte fixiert. Genau wie vor nunmehr fast 20 Jahren, als sie und ihre Zwillingsschwester Bianca wieder und wieder zu vorgeblichen Spezialbehandlungen in den berüchtigten Turm gebracht wurden. So wie alle Bewohner der Odenwaldklinik, die nach außen ein renommiertes Sanatorium für reiche psychisch gestörte Patienten war. Bis Doris und Bianca mit Hilfe eines Zivildienstleistenden die wahren Vorgänge hinter den Mauern der alten Villa an die Öffentlichkeit und so die Goldmann-Brüder für viele Jahre hinter Gitter bringen konnten. Doch nun stehen beide wieder vor ihr. Ihre Albträume sind wahr geworden, sie ist ihren früheren Peinigern wieder schutzlos ausgeliefert.

„Was wollen Sie von mir“, fragt Doris mit brüchiger Stimme, „und wo ist Bianca?“ „Deine Schwester?“ Die Frage scheint Professor Goldmann zu erheitern. „Die siehst du nie wieder! Und was ich von dir will, erfährst du morgen früh. Mach es dir bequem“, sagt Goldmann, wobei er grinsend auf die Fesseln blickt. „Du wirst noch eine ganze Weile hier sein.“ „Aber Bianca braucht mich doch! Sie kann ohne mich nicht leben!“ Tränen rinnen über Doris’ Gesicht. Höhnisch lachend drehen sich die Goldmann-Brüder um, schalten das Licht aus und schließen die Tür. Sie lassen Doris in völliger Dunkelheit zurück – allein, hilflos und in Ungewissheit. So wie früher. Alte Ängste steigen in ihr auf, Ängste, die sie längst besiegt glaubte.

Damals hatte sie sich in ihre eigene Welt geflüchtet, gemeinsam mit ihrer Zwillingsschwester. Eine Welt voller Zahlen, die allen anderen ein Rätsel blieb. Eine Welt, in der nur die Schwestern einander verstanden und zu der niemand anderes Zugang hatte – außer Martin. Martin, der Zivi, der schließlich die Behörden einschaltete und Doris und Bianca so befreite. Ob Martin ihr auch diesmal helfen kann?

Die Schwestern waren als Kinder so unzertrennlich, wie es das Klischee von Zwillingen erwartet. Sie waren die einzigen, die einander immer verstanden. So wurden sie nach der Autismus-Diagnose gemeinsam in die Odenwaldklinik eingewiesen – und trennten sich auch dann nicht, als das Sanatorium geschlossen wurde. Sie zogen einfach in eine gemeinsame Wohnung und behielten sogar trotz der schlimmen Erinnerungen ihre Zahlen-Geheimsprache bei. Sie benutzen sie nun, um sich auf der Straße über andere Leute lustig zu machen. Und um mit Martin zu chatten, der sie noch immer gelegentlich besucht, wenn er in der Nähe ist und etwas Zeit erübrigen kann.

Martin Kramer ist längst kein Zivildienstleistender mehr, der ungeduldig darauf wartet, mit seinem Informatikstudium zu beginnen. Der seltsame Dialog der Schwestern brachte ihn damals dazu, sich für Kryptografie zu interessieren – und dabei ist er auch nach Abschluss seines Studiums geblieben. Inzwischen ist er Spezialist für sichere Kommunikation in einer großen Bank und bereist Niederlassungen in der ganzen Welt. Doch ein Anruf des Betreuers der beiden Schwestern hat seine Reisepläne zunichte gemacht: Doris ist verschwunden.

* * *

Als Martin in der Wohnung der Schwestern eintrifft, ist die Polizei noch vor Ort. Von Doris fehlt jede Spur. Zuletzt hatte Bianca sie vor dem Schlafengehen gesehen. Als sie am späten Morgen noch immer nicht aufgestanden war, wollte Bianca nach ihr sehen – fand aber nur das leere Bett und im Briefkasten eine Nachricht ihrer Schwester.

Illustration: Jan Bintakies, Hannover

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

„Das ist der rätselhafteste Abschiedsbrief, den ich je gesehen habe. Keine Ahnung, was das bedeuten soll“, sagt Kommissar Altmann, als er auf ein mit vielen Zahlen beschriebenes Pik-As deutet, das Bianca in einem Umschlag im Briefkasten gefunden hat. „Ihre Schwester scheint das entziffern zu können. Leider ist nichts aus ihr herauszukriegen.“ Bianca ist völlig in Tränen aufgelöst und bekommt kein einziges Wort über die Lippen. „Ihr Betreuer hat die Schwester jedenfalls als vermisst gemeldet, er ist gerade mit meinen Kollegen auf dem Revier.“

Als Martin die Spielkarte mit neun langen Zahlen sieht, erkennt er augenblicklich das vertraute Muster. „Die Nachricht ist verschlüsselt. Haben Sie hier irgendwo noch mehr Karten gesehen?“ „Noch mehr Karten?“ „Ja, Spielkarten, auf denen ebenfalls Zahlen notiert sind. Schauen Sie mal im Bad nach, in der Nähe des Spiegels. Dort haben sie sie früher oft aufbewahrt. Ich suche hier.“

Als Kommissar Altmann zurückkehrt, hält er zwei Spielkarten in der Hand, auf denen etliche Zahlen in zwei Spalten stehen. Alle Zahlenpaare mit Ausnahme des letzten wurden fein säuberlich durchgestrichen. Martin nimmt die Karten entgegen und kniet sich vor Bianca hin: „Welche ist deine?“ Bianca deutet stumm auf die Karte mit den Zahlen 632.579 und 5; auf der anderen stehen die Zahlen 674.969 und 17. „Das ist der Schlüssel“, sagt Martin zu Kommissar Altmann, „sie ändern ihn jeden Tag.“ „So, so“, entgegnet der Kommissar ungläubig, „und wie lautet die Nachricht nun?“

WIR SPRECHEN HIER TATSÄCHLICH VON STARKER KRYPTOGRAFIE, WIE SIE SOGAR NACHRICHTENDIENSTE BENUTZEN.

Martin greift zu seinem Smartphone, gibt dort die neun Zahlen des Pik-As ein und zusätzlich die Zahlen von Biancas Spielkarte. „Da haben wir es“, sagt Martin und zeigt das Smartphone dem Kommissar:

```
ICH*GEHE*FORT*SUCHT*MICH*NICHT**INAO
```

„ ‚Sucht mich nicht‘, eindeutig ein Abschiedsbrief.“ Kaum hat Kommissar Altmann Doris’ Worte vorgelesen, springt Bianca auf und schreit dem Kommissar entgegen: „Das ist nicht wahr! Wir müssen sie finden! Sie will, dass wir sie suchen!“ „Beruhige dich, Bianca! Natürlich werden wir Doris suchen. Herr Kommissar, lassen Sie uns draußen weitersprechen.“

Als Martin die Tür geschlossen hat, spricht ihn der Kommissar an: „Herr Kramer, ich will Ihnen nichts vormachen. Wir haben einen Abschiedsbrief, zugegebenermaßen einen sehr ungewöhnlichen. Noch dazu auf einem Pik-As geschrieben, das in manchen Kreisen als Todeskarte gilt. Und wie Sie selbst sagen, kommunizieren die Schwestern auf diese merkwürdige Art, mit Zahlen auf Spielkarten. Es war doch Doris, die das schrieb?“ „Ja, es sieht ganz danach aus. Aber ich kann mir nicht vorstellen, dass sie Bianca verlassen würde. Die beiden waren noch nie länger als ein paar Stunden voneinander getrennt. Das passt nicht zu ihr.“ „Ihnen ist sicher klar, dass ich keine Hundertschaft auf die Suche nach Doris schicken kann. Aber wir werden Doris als vermisste Person zur Fahndung ausschreiben. Begleiten Sie mich bitte in mein Büro. Ich brauche Ihre Hilfe, um Doris’ Nachricht zu Protokoll zu bringen.“

* * *

„Also Herr Kramer, fürs Protokoll: Die Schwestern verständigen sich also in einer Art Geheimsprache, in der auch die Nachricht auf der Spielkarte verfasst ist?“ „Das ist keine Geheimsprache. Doris und Bianca verschlüsseln ihre Nachrichten. So, wie man E-Mails oder andere Daten verschlüsselt. Vielleicht haben Sie schon mal etwas von asymmetrischer Verschlüsselung gehört, Stichwort Public/Private Key oder RSA? Wir sprechen hier tatsächlich von starker Kryptografie, wie sie sogar Nachrichtendienste benutzen. Mit dem Unterschied, dass die Geheimdienste mit noch größeren Zahlen arbeiten als Doris und Bianca.“

„Also braucht man einen Computer, um diese Nachrichten zu entschlüsseln?“ „Unsereiner unbedingt! Doris und Bianca hingegen können das im Kopf. Eine unglaubliche Leistung, das ist ihre Begabung. Viele autistisch veranlagte Menschen haben solche sogenannten Inselbegabungen.“

„Welche Rolle spielen dabei die Spielkarten?“ „Auf denen notieren sich Doris und Bianca jeweils den öffentlichen Teil ihres Schlüssels, den sie am betreffenden Tag verwenden. Das ist Teil ihres Morgenrituals. Spielkarten benutzen sie vermutlich deshalb, weil sie im Sanatorium, in dem sie viele Jahre lebten, keine Karteikarten oder Ähnliches bekamen. Eine Bedeutung hat der Wert der Spielkarte nicht.“

Martin holt die beiden Spielkarten hervor, die Kommissar Altmann im Bad von Doris und Bianca fand: „Weil sie ein asymmetrisches Verschlüsselungsverfahren mit öffentlichem und privatem Schlüssel verwenden, hat jede Schwester einen eigenen Schlüssel, deshalb gibt es stets zwei Karten. Mithilfe des öffentlichen Schlüssels des Empfängers wird dann die Nachricht kodiert. Den privaten Teil ihres Schlüssels merken sich Doris und Bianca, er wird niemals aufgeschrieben. Ohne ihn ist es nicht möglich, die Nachricht zu entschlüsseln.“

„Aber als Sie vorhin die Nachricht von Doris mit Ihrem Smartphone entschlüsselt haben, hatte Ihnen Bianca doch gar keinen Code verraten. Sie hatten Bianca nur gefragt, welche der beiden Karten ihre sei, und diese Daten eingegeben. Das widerspricht sich doch.“ „Da haben Sie prinzipiell Recht. Schauen Sie, auf Biancas Karte stehen zwei noch nicht durchgestrichene Zahlen: 632.579 und 5. Die erste Zahl ist der sogenannte Hauptmodul, die zweite der Exponent. Beide benötigen Sie, um eine Nachricht an Bianca zu verfassen. Der Hauptmodul ist das Produkt zweier Primzahlen – und diese zwei Primzahlen sind die Basis für Ver- und Entschlüsselung.“

„Die Primfaktorzerlegung von 632.579 ist noch überschaubar“, fährt Martin fort. „Wenn Nachrichtendienste die-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

ses Verfahren nutzen, sind der Hauptmodul und die Primfaktoren sehr viel größer. Die Sicherheit des Verschlüsselungsverfahrens beruht darauf, den Hauptmodul so groß zu wählen, dass eine Primfaktorzerlegung auch mit Großrechnern in vernünftiger Zeit nicht möglich ist. Bei einer sechsstelligen Zahl wie 632.579 genügt aber schon ein Browser mit Internetzugang, um die Primfaktoren zu bestimmen. Rufen Sie doch mal die Internetseite wolframalpha.com auf und geben Sie dort ‚factor 632579' als Anfrage ein."

„Einen Moment ... das Ergebnis ist 733 und 863." „Damit kennen wir den geheimen Schlüssel. Bevor Sie die Nachricht entschlüsseln können, müssen Sie allerdings wissen, auf welche Weise diese verschlüsselt wurde. So benutzen Doris und Bianca in ihren Nachrichten lediglich die Buchstaben A bis Z und einen Wortzwischenraum. Jedem Zeichen ist ein Zahlenwert zugeordnet, ich schreibe Ihnen das mal auf."

*	0	I	9	R	18
A	1	J	10	S	19
B	2	K	11	T	20
C	3	L	12	U	21
D	4	M	13	V	22
E	5	N	14	W	23
F	6	O	15	X	24
G	7	P	16	Y	25
H	8	Q	17	Z	26

„Die Verschlüsselung erfolgt immer blockweise, es werden also mehrere Buchstaben zusammengefasst und dann erst verschlüsselt. Damit die Zahlen später nicht zu groß werden, verrechnen die Schwestern immer nur vier Buchstaben miteinander. Im ersten Schritt wurde Doris' Nachricht „Ich gehe fort sucht mich nicht" also in Vierergruppen aufgeteilt. Die erste Gruppe lautet ‚ICH*'. Wandelt man die Zeichen nach der Tabelle in Zahlen um, ergeben sich daraus die Zahlen 9, 3, 8 und 0 für den Wortzwischenraum." „Okay, das ist einfach."

„Als Nächstes hat Doris die vier Zahlen zusammengefasst. Dabei bediente sie sich desselben Tricks, mit dem man im Dezimalsystem die Zahlen 1, 2, 3 und 4 zu 1.234 zusammenfassen kann: Die ganz rechte Zahl multipliziert man mit 10^0, also 1, die zweite von rechts mit 10^1, also 10, die dritte mit 10^2, also 100, und die vierte mit 10^3, also 1.000. Und 4+30+200+1000 ergeben 1.234. Die Basis im Dezimalsystem ist 10, weil der höchste Einzelwert 9 ist."

„Bei den von Doris und Bianca verwendeten Buchstaben ist der höchste Einzelwert 26, weshalb die einzelnen Zahlen mit 27 respektive der Potenz von 27 multipliziert werden. So entsteht aus jeweils vier Buchstaben der Nachricht eine Zahl. Das sieht dann so aus:

```
ICH* → {9,3,8,0}
          → 9*27^3 + 3*27^2 + 8*27^1 + 0*27^0 = 179550
GEHE → {7,5,8,5}
          → 7*27^3 + 5*27^2 + 8*27^1 + 5*27^0 = 141647
*FOR → {0,6,15,18}
          → 0*27^3 + 6*27^2 + 15*27^1 + 18*27^0 = 4797
T*SU → {20,0,19,21}
          → 20*27^3 + 0*27^2 + 19*27^1 + 21*27^0 = 394194
CHT* → {3,8,20,0}
          → 3*27^3 + 8*27^2 + 20*27^1 + 0*27^0 = 65421
MICH → {13,9,3,8}
          → 13*27^3 + 9*27^2 + 3*27^1 + 8*27^0 = 262529
*NIC → {0,14,9,3}
          → 0*27^3 + 14*27^2 + 9*27^1 + 3*27^0 = 10452
HT** → {8,20,0,0}
          → 8*27^3 + 20*27^2 + 0*27^1 + 0*27^0 = 172044
```

„Doris und Bianca berechnen das im Kopf, Sie können einfach Wolfram Alpha dafür benutzen. Die Nachricht ist bis jetzt aber nur in Zahlen umgewandelt, die Verschlüsselung erfolgt erst im nächsten Schritt.

Dabei wird die Zahl eines Blocks mit dem Exponenten des öffentlichen Schlüssels des Empfängers potenziert. Bei einer Nachricht für Bianca ist das 5. Das ergibt eine ziemlich große Zahl, die nun noch durch Biancas Hauptmodul 632.579 geteilt wird, dann bestimmt man den Rest. Das nennt sich Modulo-Operation. Das Ergebnis ist die verschlüsselte Nachricht, wie wir sie auf dem Pik-As gefunden haben. Auch diese Rechenarbeit können Sie Wolfram Alpha erledigen lassen, in einem Schritt für die gesamte Nachricht:

```
{179550,141647,4797,394194,65421,262529,10452,172044}^5 ↵
                                              ↳ mod 632579 = ↵
↳{216009,505957,521919,583981,339002,161825,600064,627740}
```

Um den Text wieder zu entschlüsseln, benötigen Sie zunächst die beiden Primfaktoren, aus denen der Hauptmodul besteht. Bei 632.579 sind das 733 und 863, wie Ihnen Wolfram Alpha ja schon verraten hat. Damit haben Sie praktisch Biancas Schlüssel geknackt, Bianca hat diese beiden Primzahlen im Kopf.

Die Primzahlen benötigen Sie, um den Entschlüsselungsexponenten, nennen wir ihn X, zu bestimmen. X muss folgende mathematische Bedingung erfüllen, wobei n für eine ganze Zahl steht:

```
5 * X = n * (733-1)*(863-1) + 1
```

Auch hier hilft Ihnen bei der Berechnung Wolfram Alpha weiter: Geben Sie die Gleichung dort ein, so bestimmt die Suchmaschine unter anderem eine ganzzahlige Lösung (Integer Solution), die so aussieht:

```
n = 5m + 1, X = 630984m + 126197
```

Die einfachste Lösung mit dem kleinsten Entschlüsselungsexponenten X finden Sie bei m = 0, also X = 126.197. Mit diesem Wert können Sie Doris' Nachricht wieder entschlüsseln. Dazu potenzieren Sie den verschlüsselten Wert der einzelnen Blöcke mit dem Entschlüsselungsexponenten 126.197 und bestimmen den Rest, der beim Teilen durch den Hauptmodul 632.579 übrig bleibt:

```
{216009,505957,521919,583981,339002, ↵
          ↳ 161825,600064,627740}^126197 mod 632579 = ↵
  ↳{179550,141647,4797,394194,65421,262529,10452,172044}
```

Um aus den entschlüsselten Werten der Blöcke wieder Text zu machen, müssen Sie die Zahlen der einzelnen Buchstaben zurückgewinnen. Das klappt genau so wie im Dezimal-

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

system mit der Zahl 1.234: Um die zweite Ziffer von rechts zu erhalten, bestimmt man zunächst den Rest der Division durch 10^2 (mod), das sind 34, teilt das durch 10^1, was 3,4 ergibt, und nimmt dann den ganzzahligen Teil (floor), womit 3 übrig bleibt. Für die anderen Stellen der Zahl 1234 geht man ebenso vor, es ändern sich dabei nur die Zehnerpotenzen. Das gleiche Verfahren, nur mit einer Basis von 27, wenden Sie bei den entschlüsselten Textblöcken an.“

```
floor((179550 mod 27^{4,3,2,1})/27^{3,2,1,0}) = {9,3,8,0}
                                                → ICH*
floor((141647 mod 27^{4,3,2,1})/27^{3,2,1,0}) = {7,5,8,5}
                                                → GEHE
floor((4797 mod 27^{4,3,2,1})/27^{3,2,1,0}) = {0,6,15,18}
                                                → *FOR
floor((394194 mod 27^{4,3,2,1})/27^{3,2,1,0}) = {20,0,19,21}
                                                → T*SU
floor((65421 mod 27^{4,3,2,1})/27^{3,2,1,0}) = {3,8,20,0}
                                                → CHT*
floor((262529 mod 27^{4,3,2,1})/27^{3,2,1,0}) = {13,9,3,8}
                                                → MICH
floor((10452 mod 27^{4,3,2,1})/27^{3,2,1,0}) = {0,14,9,3}
                                                → *NIC
floor((172044 mod 27^{4,3,2,1})/27^{3,2,1,0}) = {8,20,0,0}
                                                → HT**
```

„Gut“, sagt der Kommissar mit deutlicher Erleichterung. „Ich weiß zwar noch nicht, warum Hauptmodul und Entschlüsselungsexponent so berechnet werden müssen, aber ich komme immerhin zu einem sinnvollen Ergebnis.“ „Das ist ja auch die Hauptsache“, entgegnet Martin. „Sollten Sie einmal genau wissen wollen, wie die Teile des Schlüssels zusammenhängen, empfehle ich Ihnen den Artikel ‚Der Dialog der Schwestern‘, der nach dem Skandal in der Odenwaldklinik vor fast 20 Jahren im Computermagazin c’t veröffentlicht wurde.“

* * *

„Aber sagen Sie, Herr Kramer, wir haben jetzt immer nur die ersten acht Zahlen des Pik-As benutzt. Was ist mit der letzten Zahl, die haben Sie doch vorhin ebenfalls auf Ihrem Smartphone eingegeben?“

„Die letzte Zahl ist eine Signatur, quasi die Unterschrift von Doris, mit der die Echtheit der Nachricht überprüft werden kann. Weil ich nicht wusste, ob die Nachricht signiert ist oder nicht, habe ich vorhin einfach alle neun Zahlen der Karte in die Entschlüsselungs-App auf meinem Smartphone eingegeben. Die Signatur berechnet sich jedoch anders als die Textblöcke, deshalb kam bei der letzten Zahl nur Buchstabensalat heraus.“

„Wir wissen durch die Signatur also mit absoluter Sicherheit, dass die Nachricht von Doris kam?“ „Das lässt sich leicht feststellen. Schauen wir uns zunächst an, wie Doris und Bianca die Signatur bilden: Dazu berechnen sie zunächst die Quersumme aller entschlüsselten Textblöcke der Nachricht. Auch so etwas erledigt Wolfram Alpha mit links.“

```
sum of digits 17955014164747973941946542126252910452172044
                                                = 181
```

„Die Signatur erhalten Sie, indem Sie die Quersumme verschlüsseln.“ „Gut. Wie das geht, habe ich ja gerade gelernt. Also 181 hoch 5 Modulo 632.579 …“ „Warten Sie. Die Signatur hat ja die Aufgabe, die Authentizität einer Nachricht zu bestätigen. Für die Verschlüsselung der Nachricht wurde Biancas öffentlich bekannter Hauptmodul und der öffentlich bekannte Exponent benutzt. Es kann also jeder Nachrichten an Bianca verschlüsseln, der ihren öffentlichen Hauptmodul und ihren Exponenten kennt.

WIR WISSEN DURCH DIE SIGNATUR ALSO MIT ABSOLUTER SICHERHEIT, DASS DIE NACHRICHT VON DORIS KAM?

Würde man zum Verschlüsseln der Quersumme ebenfalls Biancas öffentliche Schlüsselkomponenten verwenden, wäre damit lediglich bewiesen, dass der Erzeuger der Signatur die entschlüsselte Nachricht kannte und deshalb die Quersumme korrekt berechnen konnte. Wer der Urheber war, könnten Sie so aber nicht feststellen.

Deshalb hat Doris ihre eigenen Schlüsselkomponenten benutzt, um die Signatur zu erzeugen. Neben dem Hauptmodul benötigte Doris ihren Entschlüsselungsexponenten für die Berechnung – und dafür wiederum die nur ihr bekannten Primfaktoren des Hauptmoduls. Den Hauptmodul 674.969 und den Exponenten 17 finden wir auf Doris’ Karte, die Primfaktoren müssen wir wieder von Wolfram Alpha knacken lassen:

```
factor 674969 = 677*997
```

Damit und mit dem Exponenten 17 können wir den Entschlüsselungsexponenten X berechnen:

```
17 * X = n * (677-1) * (997-1) + 1
n = 17m + 3, X = 673296m + 118817
```

Für m = 0 ergibt das den Entschlüsselungsexponenten 118.817. Damit hat Doris schließlich die Quersumme verschlüsselt:

```
181^118817 mod 674969 = 651282
```

Um die Signatur zu prüfen, benötigt der Empfänger lediglich den Exponenten und den Hauptmodul des Absenders, die ja beide öffentlich sind. Dann potenziert er die verschlüsselte Signatur mit dem Exponenten und berechnet den Rest der Division durch den Hauptmodul:

```
651282^17 mod 674969 = 181
```

Stimmt das Ergebnis mit der Quersumme der entschlüsselten Nachricht überein, ist bewiesen, dass der Absender die Nachricht signiert hat.“

„Aber Herr Kramer, die letzte Zahl auf dem Pik-As lautet 282.156, nicht 651.282.“ „Wie bitte? Das kann nicht sein!“ Martin reißt dem Kommissar die Spielkarte aus der Hand. „Doris würde niemals einen solchen Fehler machen! Die

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

beiden unterhalten sich ja sogar noch im Halbschlaf verschlüsselt.“ Panisch vergleicht er die Zahl auf der Karte mit der eben berechneten Signatur auf dem Monitor des Polizeicomputers.

„Die Signatur ist invertiert! Sie ist korrekt, aber Doris hat sie von hinten nach vorn aufgeschrieben. Das meinte Bianca, als sie Sie anschrie, das sei nicht wahr. Die Nachricht bedeutet das genaue Gegenteil. Doris ist nicht freiwillig fortgegangen – und sie will, dass wir sie suchen. Das ist ein Hilferuf!“

Schweigend blickt der Kommissar von der Karte zum Bildschirm und wieder zurück. Vor gut einer Stunde waren die Zahlen noch böhmische Dörfer für ihn, doch jetzt ergibt alles einen Sinn. „Ich glaube, Sie haben Recht, Herr Kramer. Ich gebe gleich eine neue Meldung durch: Wir suchen jetzt ein Entführungsopfer.“

* * *

Doris zuckt unwillkürlich zusammen, als Professor Goldmann den Sehschlitz in der Stahltür zu ihrem unterirdischen Verlies geräuschvoll schließt. Deutlich kann sie hören, wie sich die Goldmann-Brüder vor der Tür unterhalten: „Was macht die Göre?“ „Sie sitzt am Tisch rum und kritzelt wahrscheinlich ihre Memoiren auf die Karten. Oder ihr Testament, was weiß ich.“

„Apropos Testament: Die beiden haben doch ne stinkreiche Familie und bestimmt auch schon eine Menge Kohle geerbt. Lass uns doch einfach ein paar Millionen kassieren und dann verschwinden. Ich hab schon alles da, was wir brauchen: aktuelle Tageszeitung, Sofortbildkamera, das ist in fünf Minuten erledigt. Und wen interessiert’s, was danach aus den Gören wird?“

„Mich! Sie haben mein Leben zerstört, meine Existenz, verdammt, sogar meine Approbation als Arzt! Ich weiß, du würdest für Geld sogar unsere Mutter verkaufen. Aber ich will kein Geld! Ich will Rache! Ich will sehen, wie sie getrennt und allein zugrunde gehen und sich schließlich selbst umbringen! Ich bin kein billiger Erpresser wie du! Und jetzt lass mich in Ruhe!“ Mit diesen Worten schlägt Professor Goldmann eine Tür zu und Doris hört, wie sich seine Schritte entfernen.

„Dann gibt’s halt kein Geld für dich, bleibt um so mehr für mich“, hört Doris den Bruder halblaut sagen. Sekunden später wird ein Stuhl geräuschvoll zurückgeschoben, Papier raschelt und jemand macht sich an der Stahltür zu schaffen. Blitzschnell greift Doris zu einer Karte, dem Herz-As, schreibt ein paar Zahlen darauf und kann sie gerade noch im Ärmel ihrer Strickjacke verstecken, als Professor Goldmanns Bruder den Raum betritt. „Bleib, wo du bist“, herrscht er sie an. Grob drückt er Doris die Tageszeitung in die Hand. „Festhalten! Und guck in die Kamera!“ Es blitzt, Goldmann entreißt ihr die Zeitung, dreht sich um und wirft die Stahltür hinter sich zu.

* * *

Das Smartphone hat kaum einen Ton von sich gegeben, da hat Martin auch schon abgehoben: „Hallo, Kommissar Altmann. Warten Sie, ich stelle auf Lautsprecher, damit Bianca mithören kann. Was gibt es?“ „Herr Kramer, ich brauche noch mal Ihre Hilfe. Kollegen haben mich gerade informiert, dass ein Erpresserbrief aufgetaucht ist. Man fordert zwei Millionen Euro Lösegeld. Der Brief wird gerade auf Spuren untersucht. Es war auch ein Foto von Doris dabei, wie sie eine Tageszeitung von gestern in der Hand hält. Und halb verdeckt eine Karte.“ „Wie lauten die Zahlen?“ „492.578, 463.179, 72.341, 24.568, 495.769 und 2.616.“

Als der Kommissar die Zahlen vorliest, beginnt Bianca über das ganze Gesicht zu strahlen. Bei der letzten Zahl springt sie auf, ruft „Sie ist es!“ und rennt zur Tür hinaus. Martin hat Mühe, Bianca einzuholen und unterdessen dem Kommissar die entschlüsselte Nachricht durchzugeben.

* * *

Wenige Stunden später füllt ein endloses Zahlengeplapper das kleine Doppelzimmer im städtischen Klinikum, in dem sich Doris von den Strapazen der letzten Tage erholen soll. Ihre Schwester Bianca weicht ihr nicht von der Seite. „Es ist mir unbegreiflich“, sagt Kommissar Altmann zu Martin. „Ich habe am Computer über eine Stunde gebraucht, um nur wenige Worte zu entschlüsseln.“ „Ja, es ist beeindruckend, mit welcher Geschwindigkeit sie das beherrschen – und ganz ohne Hilfsmittel.“ „Doris hatte Glück, dass sich Professor Goldmann nur dafür interessiert hat, wie die beiden Schwestern ihre Nachrichten verschlüsseln, aber nicht, wie sie sie signieren. Sonst hätte er womöglich Doris’ invertierte Signatur entdeckt.“ „Tja, man sollte eben immer erst die Signatur prüfen, bevor man einer Nachricht vertraut.“

(mid@ct.de) c't

Alle Zahlen zum Nachrechnen, der Link zur alten c’t-Story sowie das C-Listing zur Entschlüsselung: ct.de/ypgv

Von der Verschlüsselung zur Signatur

Eine c’t-Story findet nach fast 20 Jahren ihre Fortsetzung: In Heft 25/1999 erschien „Der Dialog der Schwestern“ von Carsten Elsner als Verschlüsselungskrimi und Herausforderung für Freunde mathematischer Rätsel. Damit auch neue Leser diese Vorgeschichte der aktuellen Story genießen können, haben wir sie auf ct.de/ypgv frei zugänglich gemacht. An ihrem Schluss steht ein grausiges Geheimnis, das man selbst lüften muss – mithilfe eines Taschenrechners oder eines C-Programms, das unser Leser Frank Rustemeyer seinerzeit geschrieben hat.

Jetzt sind die Schwestern, die damals Kinder waren, erwachsen geworden – ihre ungewöhnliche Art der verschlüsselten Kommunikation pflegen sie aber nach wie vor. Allerdings ist inzwischen ein zusätzliches Sicherungsmoment hinzugekommen: eine Signatur zur Authentifizierung. So spannen beide Storys einen Bogen nicht nur über zwei Jahrzehnte im Leben von Bianca und Doris, sondern auch über die praktische Entwicklung abgesicherter Kommunikation.

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover