Neues von den Schwestern

Carsten Elsner
(Revidierte Fassung von Mirko Dölle)

c't magazin für computer technik 3 (2019), 188 - 193.

Diese Erzählung ist eine Fortsetzung der in derselben Zeitschriftenreihe 1999 erschienenen Story *Der Dialog der Schwestern* (c't magazin für computertechnik **25** (1999), 288-296). In diesen Erzählungen für einen breiteren Leserkreis wird das RSA-Verfahren schrittweise entwickelt. Es ist ein Versuch, Mathematik unterhaltsam - ohne Verwendung eines Formalismus - zu vermitteln.
In der Erzählung *Der Dialog der Schwestern* von 1999 wird das RSA-Verfahren noch in einer sehr vereinfachten Form dargestellt: es wird ein Text buchstabenweise verschlüsselt, es gibt keine Signaturen, beide Schwestern benutzen bei ihren Dialogen dieselben Schlüsselbestandteile zum Ver- und Entschlüsseln, und die modulare Arithmetik ist mit einem einfachen Taschenrechner nachvollziehbar. In der Fortsetzung *Neues von den Schwestern* wird das RSA-Verfahren von den Protagonistinnen in modernerer Form verwendet: Außer einem gemeinsamen Modul benutzen beide individuelle Schlüsselbestandteile und die in Blöcke zerlegten Nachrichten werden signiert. Die dabei eingesetzten Zahlen sind nun größer, so daß die Rechnungen nur mit Computer-Algebra-Systemen effektiv nachvollziehbar sind. Hierzu wird in der Geschichte die Internetseite *wolframalpha.com* empfohlen. Die Protagonistinnen sind Autistinnen, die die einseitige Begabung ungewöhnlichen Kopfrechnens beherrschen und bei ihren verschlüsselten Dialogen auf keine technischen Hilfsmittel angewiesen sind.
Beide Erzählungen über die Schwestern sind Rätselgeschichten. Das heißt, die Auflösung der als Kriminalfälle geschilderten Ereignisse muß sich der Leser selber verschaffen, was ihm gelingt, wenn er die in die Geschichten eingebundenen Erklärungen zur Funktionsweise des RSA-Verfahrens verstanden hat. Neben den beiden Autistinnen spielt ein Martin eine besondere Rolle, der (1999) sich selber über den Dialog der Schwestern in das RSA-Verfahren einarbeitet, 2019 dann einem Kommissar (und damit dem Leser) die nötigen Informationen über die Verschlüsselungstechnik vermittelt. 1999 leben die Schwestern in einem Pflegeheim, in dem die Pflegeleitung Verbrechen an den Insassen des Heims begeht, die von Martin als Zivildienstleistendem in dem Hause aufgedeckt werden. 2019 leben die Schwestern nicht mehr in dem Sanatorium, das nach den Vorfällen vor 20 Jahren geschlossen wurde; sie sind aber nun den Racheplänen der ehemaligen Heimleitung ausgesetzt, die mittlerweile ihre Gefängnisstrafe abgesessen hat. Die Auflösung dieser neueren Geschichte basiert weniger auf der Entschlüsselung einer Nachricht, sondern auf der dieser Nachricht beigefügten korrekten Signatur.

Ein ähnlicher Ansatz zur formellosen Vermittlung von Mathematik wird auch in der Erzählung *Das chinesische Labyrinth* verfolgt (c't magazin für computertechnik **21** (2001), 308-312). Auch dies ist eine Rätselgeschichte, die den Leser zum Nachdenken anregen soll. Hier dreht sich alles um Marco Polo, der zusammen mit weiteren Bewerbern um ein Amt am Hofe des Großkhans in einem Labyrinth Aufgaben lösen muß, wobei beim Scheitern das Leben der Kandidaten bedroht scheint.