NT 19 (25.01.2010) 25

Über Codeknacker von gestern und morgen

Aus der Geschichte der Verschlüsselungskunst – Anschauliche Präsentation mit historischen Persönlichkeiten

Oberviechtach. (lg) Die verschlüsselte Weitergabe von geheimen Nachrichten hat in der Geschichte der Menschheit eine große Rolle gespielt. Und so lange es geheime Mitteilungen gibt, so lange sind auch die Codeknacker aktiv, die die chiffrierten Informationen entschlüsseln wollen. „Kryptographie" heißt der Fachbegriff für die Verschlüsselungskunst, während unter „Kryptoanalysten" die Codeknacker zu verstehen sind.

Einen Crash-Kurs in der Kunst der Verschlüsselung bekamen die Besucher des Elternforums am Ortenburg-Gymnasium geboten, als Professor Dr. Martin Kreuzer von der Fakultät für Informatik und Mathematik der Universität Paussau in die Kryptographie einführte. Oberstudiendirektor Günter Jehl stellte ihn als Studienkollege und Schachgegner vor. Seine Frau ist eine gebürtige Oberviechtacherin.

Die zahlreichen Zuhörer bekamen einen hochinteressanten Ausflug in die Geschichte der Verschlüsselungskunst geboten, sie erhielten aber auch Einblicke, wie künftige Verschlüsselungssysteme bei Computern und Banken gestaltet sein können. Der geschichtliche Rückblick führte in die Zeit 1500 v. Chr. nach Seleucia am Tigris, wo die Rezeptur für eine Glasur in einer Keilschrift-Verschlüsselung gezeigt wurde.

> Sobald der Quantencomputer entwickelt ist, können Sie wieder mit dem Papierzettel zur Bank gehen!
>
> Professor Dr. Martin Kreuzer

Für den kurzweiligen Vortrag bedankte sich Schulleiter Günter Jehl (links) bei Professor Dr. Martin Kreuzer (Mitte), der in seiner Präsentation auch historische Persönlichkeiten auftreten ließ. Bild: lg

Als „ersten Code-Knacker der Geschichte" stufte der Referent den Propheten Daniel ein, der Belsazars Menetekel („Gezählt – Gewogen – Geteilt") deutete. Interessant war auch der Code der Spartaner 475 v. Chr., wo aus einem Schriftband mit Buchstaben nur ein sinnvoller Text herauskam, wenn man beim Aufrollen einen Holzstab von bestimmter Dicke verwendete.

Zur Überraschung der Zuhörerschaft benannte Professor Kreuzer nicht nur geschichtliche Persönlichkeiten, die sich der Verschlüsselungskunst bedienten, sondern er ließ sie auch auftreten. So hat Cäsar in seinen geheimen Botschaften einen relativ einfaches Code-System angewendet, bei dem die Buchstaben um drei Stellen verschoben wurden. Statt einem A verwendete er z.B. ein C.

Nach Cäsar ließ der Referent auch Casanova und Kaiserin Maria Theresia auftreten. Mitarbeiter am „Lehrstuhl für Symbolic Computation", so die offizielle Bezeichnung von Kreuzers Lehrstuhl, schlüpften in diese Rollen und bewiesen, dass Naturwissenschaftler auch exzellente Schauspieler sein können. In so genannten „Schwarzen Kammern" von Maria Theresias Geheimer Staatskanzlei wurden im Wien des 18. Jahrhunderts die Briefe der Botschaften geöffnet und die Codes der verwendeten Geheimschriften geknackt.

Ein erstes Codeknacker-Buch wurde bereits 850 in Bagdad veröffentlicht. Das erst 1987 wieder entdeckte Buch wendete bereits ein Dechiffrierverfahren an, das in seinem Grundprinzip bis heute praktiziert wird, nämlich die Häufigkeitsanalyse. Die Entschlüsselung orientiert sich an der Häufigkeit der Buchstaben bzw. Symbole. Üppige Codebücher mit einer Nomenklatura an Wortersetzungen gab es beispielsweise unter dem Antipapst Clemens VII. in Avignon. Eine Weiterentwicklung ist in der „polyalphabetischen Verschlüsselung" zu sehen, wo mit Hilfe einer Verschlüsselungsscheibe gearbeitet wurde. Je nach Stellung der Scheibe werden die Buchstaben unterschiedlich verschlüsselt. Blaise de Vigenière gab eine Sammlung aller bekannten Kryptosystheme heraus. Einer der genialsten Codeknacker des Viktorianischen Zeitalters war Charles Babbage, der den „ersten mechanischen Computer" gebaut hat.

Der so genannte RSA-Schlüssel, benannt nach den Anfangsbuchstaben der drei Erfinder Rivest, Shamir und Adleman funktioniert nach den System des Mathematikers Euler. Diese Codierung wurde in den siebziger Jahren entwickelt und ist die Grundlage der heutigen Verschlüsselungssysteme, etwa beim Online-Banking. In seinem Ausblick verwies Kreuzer auf die Quantenkryptographie. „Sobald der Quantencomputer entwickelt ist, können Sie wieder mit dem Papierzettel zur Bank gehen!", lautete seine Warnung. Aber wenn es so weit ist, „werden Mathematiker, Informatiker oder Quantenpyhsiker die Menschheit retten".