Drucken

Klaus Schmeh

Doppelwürfel entschlüsselt

Israeli knackt scheinbar unlösbares Jahrhunderträtsel

Dienstag, 17.12.2013, 18:14 · · von FOCUS-Online-Experte Klaus Schmeh (Kryptologe)

Vergrößern
Teilen und Details
Colourbox.de Der „Doppelwürfel“ gilt als das beste Verschlüsselungsverfahren, das sich alleine mit Papier und Stift ausführen lässt

Ein israelischer Computer-Experte hat eine Verschlüsselung geknackt, die Experten für unlösbar hielten. Für sie war es ein Jahrhunderträtsel. Wie George Lasry den Doppelwürfel entschlüsselt hat und wie diese Methode funktioniert, erklärt Klaus Schmeh.

Der „Doppelwürfel“ gilt als das beste Verschlüsselungsverfahren, das sich alleine mit Papier und Stift ausführen lässt. Selbst ein Laie kann es innerhalb von Minuten lernen – und doch ist eine Doppelwürfel-Verschlüsselung selbst für einen Profi-Codeknacker eine echte Herausforderung. Kein Wunder, dass im Kalten Krieg kaum ein Geheimdienst auf dieses Verfahren verzichtete. Vor allem Spione nutzten den Doppelwürfel als unauffällige

Verschlüsselungsmethode – mit einem Verschlüsselungsgerät hätte sich ein Agent schnell verdächtig gemacht.

Der Doppelwürfel ist einfach zu erklären. Zunächst benötigt man ein Schlüsselwort, beispielsweise FOCUS. Unter dieses wird zeilenweise der Klartext (zum Beispiel ICH BIN EIN BERLINER) geschrieben:

FOCUS

ICHBI
NEINB
ERLIN
ER

Nun werden die Spalten so vertauscht, dass die Buchstaben des Schlüsselworts alphabetisch sortiert sind:

CFOSU

HICIB
INEBN
LERNI
ER

Das Ergebnis der Verschlüsselung (Geheimtext) wird nun spaltenweise ausgelesen. Es lautet in diesem Fall HILINEECERRIBNBNI. Dieses Prozedere wird anschließend mit einem zweiten Schlüsselwort wiederholt – und fertig ist die Doppelwürfel-Verschlüsselung. Im Kalten Krieg waren Schlüsselwörter mit mehr als 20 Buchstaben üblich – das war damals nicht zu knacken. Dabei gab es jedoch einige Fallstricke. So durften die beiden Schlüsselwortlängen keine gemeinsamen Teiler haben und außerdem keine Teiler der Klartextlänge sein.

Die Challenge

Doch ist der Doppelwürfel im Zeitalter des Computers immer noch sicher? Otto Leiberich, bis 1992 Leiter der Zentralstelle für das Chiffrierwesen (und damit der oberste Staatskryptologe der Bundesrepublik), hält bis heute hohe Stücke auf das Verfahren. Bereits in den Neunzigern regte er an, den Doppelwürfel zu erforschen. Er schlug vor, einen Text damit zu verschlüsseln und diesen der Fachwelt als kryptologisches Rätsel zur Verfügung zu stellen.

Leiberichs Wunsch kam ich gerne nach. 2007 verschlüsselte ich eine Nachricht bestehend aus 599 Buchstaben mit dem Doppelwürfel – die „Doppelwürfel-Challenge“ war geboren. Das Rätsel veröffentlichte ich in mehreren Artikeln und Büchern. In meinem Buch „Nicht zu knacken“ beschrieb ich die Doppelwürfel-Challenge als eines von zehn Jahrhunderträtseln der Verschlüsselungstechnik – nach Vorbild der mathematischen Millenium-Probleme. Schade nur, dass ich keine Millionenprämie für das Lösen eines der Rätsel in Aussicht stellen konnte.

Auch das Web-Portal MysteryTwister C3, auf dem kryptologische Rätsel vorgestellt werden, nahm die Doppelwürfel-Challenge auf. Dort ist auch der Geheimtext abrufbar.

Tatsächlich beschäftigten sich in der Folgezeit einige Experten mit der Doppelwürfel-Challenge und versuchten, den Code zu knacken. Otto Leiberich und ich gingen jedoch davon aus, dass dies nicht gelingen würde – selbst mit dem stärksten Computer erschien es zu aufwendig, die von zwei über 20 Buchstaben langen Schlüsselwörtern abhängigen Verwürfelungen zu entwirren.

 Drucken

Fotocredits:

Colourbox.de, FOL/Privat