Die Codemaker haben gewonnen

Bei Heise liest man: zum Thema „Internet-Anwender sind Verschlüsselungsmuffel“: „Zwar sind alle Kryptosysteme mit genügend Rechenkraft knackbar…“ Ach ja?

Wikipedia: „Das One-Time-Pad (Abkürzung: OTP, deutsch: Einmalverschlüsselung oder Einmalschlüssel-Verfahren, wörtlich Einmal-Block, nicht zu verwechseln mit dem Einmal-Passwort-Verfahren) ist ein symmetrisches Verschlüsselungsverfahren zur geheimen Nachrichtenübermittlung. Kennzeichnend ist, dass ein Schlüssel verwendet wird, der so lang ist wie die Nachricht selbst. Es ist die einzige kryptographische Methode, welche informationstheoretisch sicher ist und nachweislich nicht gebrochen werden kann – vorausgesetzt, sie wird bestimmungsgemäß verwendet.“

Und wie zum Teufel soll jemand Public-Key-Verfahren knacken?

Otto Leiberich, ehemaliger Leiter des Bundesamtes für Sicherheit in der Informationstechnik, sagt: ‚Das Wettrennen der Codemaker mit den Codebreakern ist entschieden, die Codemaker haben gewonnen. („Vom diplomatischen Code zur Falltürfunktion – Hundert Jahre Kryptographie in Deutschland, in: Spektrum der Wissenschaft, 6/99, S. 26 ff.“)

Der Satz des Artikels ist so einfach falsch und irreführend. Und Heise sollte sich bei dem Thema bedeckt halten: Mir ist kein Redakteur bekannt, mit dem man verschlüsselt kommunizieren kann und auch kein einziger öffentlicher Schlüssel, der auf irgendeiner Website des Heise-Verlags angeboten würden.