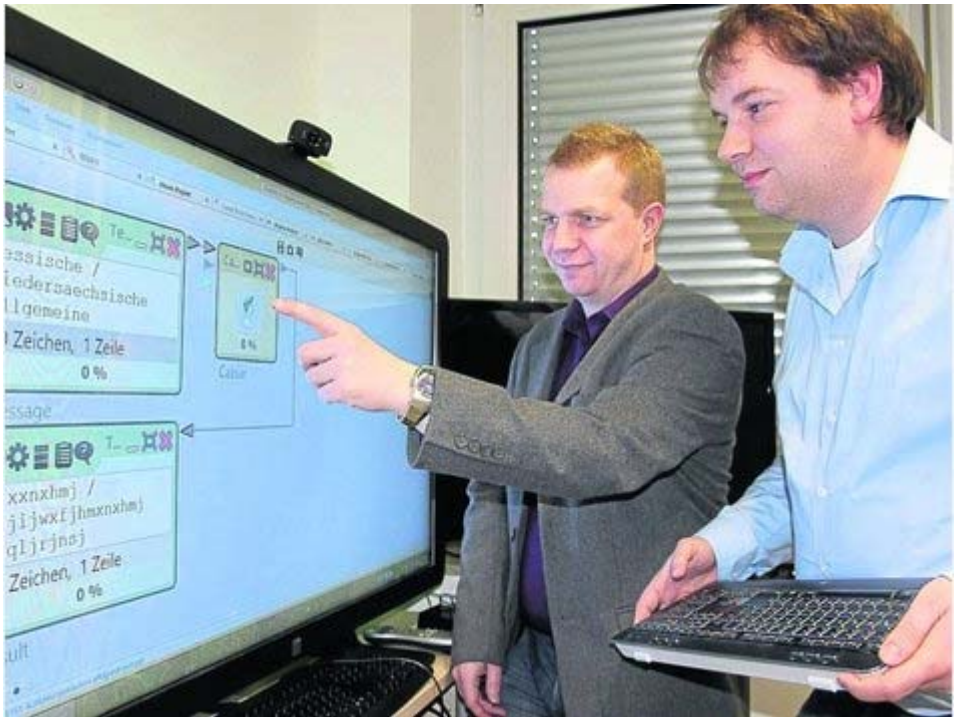
Artikel publiziert am: 24.03.2013 - 18.32 Uhr
Artikel gedruckt am: 01.05.2014 - 00.13 Uhr
Quelle: http://www.hna.de/lokales/uni/uni-kassel/knacken-geheimcodes-2818530.html

Software entschlüsselt kodierte Textbotschaften

Kasseler Informatiker knacken Geheimcodes

Kassel. Funksprüche, vertrauliche Nachrichten, Internetprotokolle: Geht es um sensible Daten, setzen Menschen seit jeher auf Geheimsprache. An der Uni Kassel können solche Codes geknackt werden:



© Foto: Schaffner

Wenn das Julius Caesar wüsste: Professor Arno Wacker (links) und Nils Kopal entschlüsseln mithilfe des Computerprogramms CrypTool 2.0 die Geheimsprache des römischen Feldherrn in Sekundenbruchteilen.

Der Kasseler Informatik-Professor Arno Wacker hat ein Computerprogramm mitentwickelt, mit dem man Einblicke in die Wissenschaft der geheimen Botschaften bekommt – und verschiedene Geheimsprachen dekodieren kann.

Ihren Ursprung hat die Software „CrypTool 2.0“ in einem Schulungsprojekt für IT-Sicherheitsexperten der Deutschen Bank. Ein Forscherteam um Prof. Wacker entwickelt seit 2007 einen Nachfolger, „der alle Menschen ansprechen soll, die sich für Kryptologie interessieren“, sagt der Leiter des Fachgebiets Angewandte Informationssicherheit. Deshalb ähnele die Bedienung der Software gängigen Windows-

Programmen. Und sie ist kostenlos.

CrypTool kennt derzeit etwa 40 moderne und klassische Verschlüsselungstechniken. Sie werden meist durch studentische Abschlussarbeiten eingepflegt. „Wenn man einen Text entschlüsseln möchte, kann das Programm aber auch helfen, indem es automatisch alle ihm bekannten Schlüssel ausprobiert“, sagt Nils Kopal, der das Entwicklerteam koordiniert.

Dies ist aber nur bei einigen Techniken möglich. Moderne Verfahren verwenden so viele Schlüssel, dass selbst alle Computer weltweit damit überfordert wären.

Zu den einfachsten Verschlüsselungstechniken zählt „Caesar“, die auf den gleichnamigen römischen Feldherrn zurückgeht. „Julius Caesar hat einfach die Buchstaben im Alphabet verschoben“, erklärt Kopal. Wählte er den Verschiebewert drei, wurde aus A ein D, und aus „Rom“ wurde „Urp“.

Das mag ausgereicht haben, um den Galliern Informationen zu verheimlichen, sagt Wacker. „Heute reicht das natürlich nicht mehr.“ CrypTool knacke die Methode in Sekundenbruchteilen, da es genauso viele Schlüssel wie Buchstaben gibt, also 26.

Kaum mehr Zeit benötigt das Programm für Kodierungen der Chiffriermaschine Enigma. Bekanntheit erlangte diese deutsche Rotor-Schlüsselmaschine im Zweiten Weltkrieg. Enigma vertauscht auch Buchstaben, verwendet jedoch mithilfe eingebauter Rotoren für jeden Buchstaben einen anderen Schlüssel. „Die Rotoren drehen sich nach jedem Buchstaben und bestimmen dadurch den neuen Schlüssel“, erklärt Wacker. So ergibt sich eine 24-stellige Schlüsselanzahl. Alliierte Kryptologen knackten die Enigma-Funksprüche trotzdem.

Suche nach dem Schlüssel

Heute werden sensible Daten im Internet mit dem Advanced Encryption Standard (AES) verschlüsselt. „Bei diesem Verfahren werden Buchstaben in Bits zerlegt, die in mehreren Stufen unter Verwendung eines Schlüssels bearbeitet werden“, sagt Wacker. Rechnerisch sei so eine 78-stellige Schlüsselanzahl möglich. „Derzeit ist kein praktikabler Weg bekannt, AES zu knacken“, sagt Wacker. Das gilt zumindest solange, bis jemand das Gegenteil beweist.

Von Sebastian Schaffner
