RSA Data Security: DES-Schlüssel gebrochen

Einem Team von rund 22 000 Teilnehmern ist es nach 39 Tagen gelungen, eine mit dem führenden Verschlüsselungsverfahren DES (Data Encryption Standard) chiffrierte Nachricht zu entschlüsseln. Weltweit über 50 000 Rechner waren in den letzten Wochen auf der Suche nach dem richtigen 56-Bit-Schlüssel. Damit wird eine Prämie von 5 000 Dollar fällig, die das kalifornische Krypto-Unternehmen RSA Data Security zur Belohnung ausgelobt hatte. Hätten die über das Distributed Net (http://www.distributed.net/) organisierten Amateur-Cracker den richtigen Schlüssel bereits innerhalb von 22,5 Tagen entdeckt, hätten sie das doppelte Preisgeld erhalten. Die entschlüsselte Nachricht lautet "Many hands make light work" - offensichtlich eine freundliche Geste gegenüber den weltweit tätigen Hobby-Knackern. Mit dem Wettbewerb soll gezeigt werden, daß gängige Verschlüsselungsverfahren keinen ausreichenden Schutz gegen Attacken bieten und insbesondere die nach amerikanischen Exportbestimmungen lieferbaren 40-Bit-Schlüssel leicht zu knacken sind. Mehr zu den Hintergründen des Wettbewerbs und der Ablösung von DES durch einen Nachfolgestandard lesen Sie in CHIP 4/98 (ab Seite 268), die Sie ab 9. März am Kiosk finden.

[zur Übersicht]