

# Starke Kryptographie Segen oder Fluch?

Johannes Nicolai  
johannes\_nicolai@tiscalinet.de

# Stellen Sie sich vor ...

Sie wären bei Ihrer Oma zum Kaffee eingeladen

# Omas Meinung

„Kryptographie ist doch DAS Werkzeug für Terroristen, um ihre Angriffe zu verschleiern.“

„Verbrecher können nicht mehr wirksam verfolgt werden, da die Polizei die Nachrichten nicht mehr entschlüsseln kann.“

# Stammtischargumente

„Aufrechte Menschen haben nichts zu verbergen.“

„Die erlaubten Verfahren reichen für unsere Zwecke vollkommen aus.“

„Wofür braucht man überhaupt Kryptographie?“

# Begriffsklärung

- Kryptographie: Wissenschaft, welche sich mit der Ver- und Entschlüsselung von Nachrichten, sowie der Authentifikation von Personen beschäftigt.
- Verschlüsselung: Transformation einer Nachricht mittels eines Schlüssels in einen Chiffre, was nur der Empfänger mit Hilfe des Schlüssels lesen (entschlüsseln) kann.

# Begriffsklärung

- Schlüssel: Nur mit ihm ist die Entschlüsselung möglich.
- Schlüsselstärke: Je länger der Schlüssel (wird in Bit angegeben), desto schwieriger ist es, die Verschlüsselung zu „knacken“.
- „Knacken“: Entschlüsselung ohne Kenntnis des Schlüssels, z.B. durch „Brute Force“.

# Begriffsklärung

- Brute Force: Ausprobieren aller möglichen Schlüssel, bis sich ein Erfolg einstellt.
- Starke Kryptographie: Der Brute Force Angriff dauert länger, als dass die Nachricht einen Wert hätte.
- Starke Schlüssellängen: 2048 Bit asymmetrisch, 128 Bit symmetrisch

# Reicht das aus?

- 128 Bit:  $2^{128}$  mögliche Schlüssel
- Alter des Universums:  $2^{34}$  Jahre
- Blitz + Lottogewinn am selben Tag:  $1/2^{55}$
- Atome im Universum:  $2^{265}$
- Ausdehnung des Universums:  $2^{280} \text{ cm}^3$

# Nutzen von Kryptographie

- Wahrung der Intim- und Privatsphäre
- Wahrung der Identität
- Sicherung geschäftskritischer Daten
- Schutz geistigen Eigentums
- Rechtssicherheit im Internet

# Bedeutung der eigenen Identität und Privatsphäre

- Wer Identität eines anderen aushorchen kann, kann diese Identität auch im Internet annehmen.
- Für die Folgen ist das Opfer verantwortlich. (z. B. Online Banking)

# Starke / schwache Kryptographie

„Es gibt eigentlich nur 2 Arten von Kryptographie: die eine hält Ihre kleine Schwester davon ab, Ihre Dateien zu lesen, während die andere selbst einflussreichen Regierungen den Zugang zu Ihren Dateien verwehrt.“

- Bruce Schneier, angesehenener Kryptoexperte

# Stammtischargument 2

<b><i>Kosten</i></b>	<b><i>40</i></b>	<b><i>56</i></b>	<b><i>64</i></b>	<b><i>128</i></b>
10 T. €	2 s	35 h	1 J	$10^{19}$ J
1 Mill. €	0,2 s	3,5 h	37 T	$10^{18}$ J
10 Mill. €	0,02 s	21 min	4 T	$10^{17}$ J
100 Mill. €	2 ms	0,2 min	9 h	$10^{16}$ J
1 Mrd. €	0,02 ms	13 s	1 h	$10^{15}$ J
10 Mrd. €	2 mikros	1 s	5,4 min	$10^{14}$ J

# Bedenken gegenüber starker Kryptographie

- Kryptographie sei das Werkzeug der Terroristen um Angriffe zu planen und geheim zu halten.
- Der Staat verliere so die Kontrolle über seine Bürger und sei der Kriminalität hoffnungslos ausgeliefert.

# Artikel 10 GG

„Die vertrauliche, unbeobachtete Kommunikation ist unverletzlich.“

Niemand will einen Orwellschen Überwachungsstaat.

# Praktische Hürden

- Steganographie ist zur Tarnung von Informationen wesentlich effektiver.
- Es ist fast unmöglich, herauszufinden, ob ein Datenstrom verschlüsselt ist.
- Die immense Datenflut des Internets ist gar nicht zu bewältigen.

# Wirtschaftliche Gründe

- Unternehmen wären gegen Industriespionage nicht mehr gewappnet.
- Deutschland würde den Anschluss in der kryptographischen Entwicklung verlieren.

# Zu guter Letzt

- Jede Wissenschaft hat ihre Schattenseiten (Chemie, Atomphysik, Metallurgie)
- Kryptographie ist nicht die Ursache von Verbrechen.
- Terroristen werden nicht durch Verbote abgeschreckt, die leichter wiegen als ihre eigentliche Straftat.

# Fazit

- Starke Verschlüsselung ist legitimes Mittel, die Datenschutzinteressen von Bürgern und Wirtschaft zu wahren.
- Verbot würde nicht Probleme lösen, die man mit starker Kryptographie in Verbindung bringt.

# Dankeschön für Ihre Aufmerksamkeit

- Umfangreicher Artikel mit weiteren Pro- und Kontraargumenten unter

<http://myhpi.de/~nicolai>