

Vor- und Nachteile starker Kryptographie

Gliederung (Einleitung, Hauptteil, Schluss, Rede dialektisch)

1. Einleitung
2. Begriffsklärung
3. Nutzen von Kryptographie
4. Bedeutung von „Privatsphäre“ und „Identitätswahrung“
5. Schwächen derzeitiger erlaubter Verfahren
6. Möglichkeiten starker Kryptographie
7. Bedenken gegenüber starker Kryptographie
8. Proargumente
9. Schluss

1. Einleitung

- Kaffee trinken bei Oma
- Einwände gegen derzeitige Tätigkeit (verschlüsselte Handykommunikation)
- Meinung von Freunden ähnlich, Nennung der Kontraargumente
- Reflektion, ob etwas moralisch vertretbares entwickelt wird

2. Begriffsklärung

- Kryptographie
- starke Kryptographie
- Schlüssellängen
- Größenvorstellung vermitteln:
- Blitz pro Tag: 2^{33}
- Alter Universum: 2^{34}
- Blitz + Lotto pro Tag: 2^{55}
- Atome Universum: 2^{265}
- Ausdehnung Universum: 2^{280}

3. Nutzen von Kryptographie

- Wahrung Intim- Privatsphäre (Liebesbriefe, Neigungen, ärztliche Daten, Geheimnisse, peinliche Details)
- Wahrung der Identität (Verlust guter Ruf, gläserner Mensch nach Orwell, Werbeattacken, gezielte Manipulation)
- Sicherung geschäftskritischer Daten (Strategien, Kundendaten, finanzieller Ruin, Existenzbedingung)
- Schutz von geistigem Eigentum (digitale Bilder, Schriften, Quellcode, Musik, Videos)
- Rechtssicherheit im Internet

4. Bedeutung der eigenen Identität und Privatsphäre

- wer Identität aushorchen kann, kann diese Identität selbst annehmen
- für Folgen ist man selbst verantwortlich (zum Beispiel Online Banking)

5. / 6. Schwache / Starke 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 in „Angewandte Kryptographie“

Kosten	40	56	64	128
100000	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

7. Bedenken gegenüber starker Kryptographie

- Kryptographie Werkzeug Terroristen um Angriffe zu planen und geheim zu halten
- Staat verliert die Kontrolle über Bürger und ist der Kriminalität hoffnungslos ausgeliefert
- unnötig, da vorhandene Mittel vollkommen ausreichen würden
- Aufrichtige Menschen haben nichts zu verbergen

8. Proargumente

- Artikel 10 GG, Orwellscher Überwachungsstaat nicht gewünscht
- Datenflut heute gar nicht mehr zu bewältigen
- Steganographie ist viel wichtiger
- Deutschland verliert den Anschluss in kryptographischen Gebieten
- Unternehmen und die Wirtschaft würden gegen Industriespionage nicht mehr gewappnet sein
- fast jede Erfindung des Menschen hat ihre Schattenseiten und wurde missbraucht (Pflanzenheilkunde, Chemie, Messer, Waffenproduktion, Kernspaltung, Fluchtautos)
- Kryptographie ist nicht die Ursache von Verbrechen
- Verbote würden durch Terroristen nicht beachtet werden, nur der ehrliche Bürger würde entmündigt werden (Privatsphäre, Identitätsverlust, Spielball von Unternehmen), Bürgerrecht wird aberkannt

9. Schluss

- 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.
- Rückverweis auf Einleitung (nun Argumente für Oma)