Einschub: Kryptoregulierung

- Gesetzliche Beschränkung der Nutzung kryptographischer Verfahren
  - Motivation: Verbrechensbekämpfung
  - Ganz verbieten würde zu wirtschaftlichen Nachteilen führen, deshalb: Schlüsselhinterlegung (*key escrow*)

- Gegenargumente:
  - Zentral hinterlegte Schlüssel sind attraktives Angriffsziel
  - Arbeitsgrundlage u.a. für Ärzte, Journalisten, ...
  - Verbindlichkeit elektronischer Signaturen würde in Frage gestellt
  - In Deutschland: Verfassungsrechtliche Bedenken - Grundrechte auf
    - (wirtschaftliche) Entfaltungsfreiheit (aus Art. 12 Abs. 1 GG)
    - Vertraulichkeit der Kommunikation (aus Art. 10 GG)
    - informationelle Selbstbestimmung (aus Art. 2 Abs. 1 GG)

Kryptoregulierung: Internationale Regelungen

- OECD-Richtlinien
  - empfehlen unbeschränkte Entwicklung und Nutzung kryptographischer Produkte und Dienste;
  - lehnen Key-escrow-Verfahren ab.
- Waasenaar-Gruppe (Nachfolger von COCOM - coordinating committee on multilateral export controls)
  - Abkommen von 1998 regelt Exportbeschränkungen für dual-use goods (hier: militärisch und zivil nutzbare Güter) in 33 Ländern.
  - Einschränkungen für Hard-/Softwareprodukte mit Schlüssellänge ab 56 Bits.
  - Ausnahmen: Verfahren für elektronische Signaturen und Authentifizierung.
  - Jedes Land entscheidet selbst, welche Produkte exportiert werden dürfen.
    - EU: Keine Exportbeschränkungen für Produkte des Massenmarkts.
    - USA:
      - bis 1998: Exportverbot ab Schlüssellänge > 40 Bits
      - 1998 - 2000: Freier Export in 45 Länder, u.a. Deutschland
      - seit 2000: Nur noch Begutachtungsprozess bei Schlüssellänge >64 Bits

Kryptopolitik in Deutschland

- Entwicklung, Herstellung, Vermarktung und Nutzung von Verschlüsselungsverfahren *innerhalb von Deutschland* ohne Restriktionen.
- Export von Verschlüsselungstechnik ist prinzipiell genehmigungspflichtig.
  - Vorgehen:
    - Außenwirtschaftsverordnung fordert Antrag auf individuelle Ausfuhrgenehmigung beim Bundesausfuhramt (BAFA).
    - Abstimmung dieser Anträge mit dem BSI.
    - Ausschlaggebend sind Empfänger und Zweck.
  - Ausnahmen:
    - Keine Exportrestriktionen innerhalb der Europäischen Union.
    - Keine Exportkontrolle bei elektronischen Signaturen und Authentifizierungsverfahren für die Anwendungsbereiche Banking, Pay-TV, Copyright-Schutz und schnurlose Telefone (ohne Ende-zu-Ende-Verschlüsselung).

Einschub: One-Time Pads

- Bei richtiger Verwendung „unknackbare“ Verschlüsselung (Claude Shannon 1949)
- Schlüssel
  - ist (mindestens) genauso lang wie der Klartext,
  - ist zufällig („*truly random*“) gewählt, und
  - wird niemals wiederverwendet.
- XOR-Verknüpfung von Klartext- mit Schlüssel-Zeichen.
- Praktische Einschränkungen:
  - Schlüsselmanagement extrem aufwendig
    - Großer Bedarf an „echte“ Zufallszahlen nicht einfach zu decken.
    - Alice und Bob müssen Schlüssel sicher untereinander austauschen.
  - Keine implizite Integritätssicherung (Angreifer modifiziert Ciphertext, so dass sich bei der Entschlüsselung ein sinnvoller anderer Plaintext ergibt)

Nicht überall, wo AES draufsteht, ist auch AES drin :)

- Recherchen im Heise-Verlag 12/2008

- Hersteller bewirbt Festplatte mit Hardware-AES-Verschlüsselung.
- In Wirklichkeit wird jeder Sektor der Festplatte mit demselben 512-Byte-Block XOR-verschlüsselt.
- Triviale Rekonstruktion des 512-Byte-Schlüssels möglich: „*Aufschrauben des Gehäuses dauert länger als Knacken der Verschlüsselung.*“

- `http://www.heise.de/security/artikel/Verschusselt-statt-verschluesselt-270058.html`