DuD
Datenschutz und Datensicherheit

Advanced Encryption Standard (AES)

Dirk Fox

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Im Jahre 1977 wurde der „Data Encryption Algorithm" (DEA) vom „National Bureau of Standards" (NBS, später „National Institute of Standards and Technology" – NIST) zum amerikanischen Verschlüsselungsstandard für Bundesbehörden erklärt [NBS_77]. 1981 folgte die Verabschiedung der DEA-Spezifikation als ANSI-Standard „DES" [ANSI_81].

Die Empfehlung des DES als Standard-Verschlüsselungsverfahren wurde auf fünf Jahre befristet und 1983, 1988 und 1993 um jeweils weitere fünf Jahre verlängert. Derzeit liegt eine Neufassung des NIST-Standards vor [NIST_99], in dem der DES für weitere fünf Jahre übergangsweise zugelassen sein soll, aber die Verwendung von Triple-DES empfohlen wird: eine dreifache Anwendung des DES mit drei verschiedenen Schlüsseln (effektive Schlüssellänge: 168 bit) [NIST_99].

Der DES basiert auf einer von Horst Feistel bei IBM entwickelten Blockchiffre („Lucipher") mit einer Schlüssellänge von 128 bit. Da die amerikanische „National Security Agency" (NSA) dafür gesorgt hatte, daß der DES eine Schlüssellänge von lediglich 64 bit besitzt, von denen nur 56 bit relevant sind, und spezielle Substitutionsboxen (den „kryptographischen Kern" des Verfahrens) erhielt, deren Konstruktionskriterien von der NSA nicht veröffentlicht wurden, war das Verfahren von Beginn an umstritten. Kritiker nahmen an, daß es eine geheime „Trapdoor" in dem Verfahren gäbe, die der NSA eine Online-Entschlüsselung auch ohne Kenntnis des Schlüssels erlauben würde.

Zwar ließ sich dieser Verdacht nicht erhärten, aber sowohl die Zunahme von Rechenleistung als auch die Parallelisierung von Suchalgorithmen machen heute eine Schlüssellänge von 56 bit zum Sicherheitsrisiko. Zuletzt konnte 1998 mit einer von der „Electronic Frontier Foundation" (EFF) entwickelten Spezialmaschine mit 1.800 parallel arbeitenden, eigens entwickelten Krypto-Prozessoren ein DES-Schlüssel in einer Rekordzeit von 2,5 Tagen gefunden werden.

Um einen Nachfolger für den DES zu finden, kündigte das NIST am 2. Januar 1997 die Suche nach einem „Advanced Encryption Standard" (AES) an. Ziel dieser Initiative ist, in enger Kooperation mit Forschung und Industrie ein symmetrisches Verschlüsselungsverfahren zu finden, das geeignet ist, bis weit ins 21. Jahrhundert hinein amerikanische Behördendaten wirkungsvoll zu verschlüsseln. Dazu wurde am 12. September 1997 ein offizieller „Call for Algorithm" ausgeschrieben.

An die vorzuschlagenden symmetrischen Verschlüsselungsalgorithmen wurden die folgenden Anforderungen gestellt:

- nicht-klassifiziert und veröffentlicht,
- weltweit lizenzfrei verfügbar,
- effizient implementierbar in Hard- und Software,
- Blockchiffren mit einer Blocklänge von 128 bit sowie
- Schlüssellängen von 128, 192 und 256 bit unterstützt.

Auf der ersten „AES Candidate Conference" (AES1) veröffentlichte das NIST am 20. August 1998 eine Liste von 15 vorgeschlagenen Algorithmen und forderte die Fachöffentlichkeit zu deren Analyse auf. Die Ergebnisse wurden auf der zweiten „AES Candidate Conference" (22.-23. März 1999 in Rom, AES2) vorgestellt und unter internationalen Kryptologen diskutiert.

Die Kommentierungsphase endete am 15. April 1999. Auf der Basis der eingegangenen Kommentare und Analysen wählte das NIST fünf Kandidaten aus,[1] die es am 9. August 1999 öffentlich bekanntmachte:

- MARS (IBM)
- RC6 (RSA Lab.)
- Rijndael (Daemen, Rijmen)
- Serpent (Anderson, Biham, Knudsen)
- Twofish (Schneier, Kelsey, Whiting, Wagner, Hall, Ferguson).

[1] Die Auswahlgründe wurden vom NIST in einem „Round 1 Report" publiziert (siehe „http://www.nist.gov/aes").

In einer zweiten Review-Periode werden diese fünf Kandidaten nun einer intensiveren Analyse unterzogen. Kryptologen und Experten sind aufgefordert, bis zum 15. Mai 2000 weitere Analyseresultate zu (mindestens) den folgenden Kriterien vorzulegen: Kryptoanalyse, Urheberrechtsaspekte, vergleichende Analyse und Implementierungsaspekte. Zur Diskussion der Ergebnisse wird das NIST vom 13.-14. April 2000 die dritte „AES Candidate Conference" (AES3) in New York durchführen.

Anschließend wird das NIST aus den fünf genannten Algorithmen einen oder mehrere auswählen und als „Proposed Federal Information Processing Standard" (FIPS) veröffentlichen. Nach einer letzten Review-Phase soll die Standardisierung dann im Sommer 2001 abgeschlossen werden.

Literatur

[ANSI_81] American National Standards Institute (ANSI): *Data Encryption Algorithm*. ANSI X3.92, 1981.

[NBS_77] National Bureau of Standards (NBS): *Data Encryption Standard (DES)*. Federal Information Processing Standards Publication (FIPS-PUB) 46-1, US Department of Commerce, Jan. 1977.

[NIST_99] National Institute of Standards and Technology (NIST): *Data Encryption Standard (DES)*. Federal Information Processing Standards Publication 46-3 (FIPS-PUB), 1999, to be approved.