Advanced Encryption Standard

aus Wikipedia, der freien Enzyklopädie

Der **Advanced Encryption Standard** (**AES**) ist ein symmetrisches Kryptosystem, welches als Nachfolger für DES bzw. 3DES im Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard bekannt gegeben wurde. Nach seinen Entwicklern Joan Daemen und Vincent Rijmen wird er auch *Rijndael*-Algorithmus genannt (gesprochen wie dt. "Rheindahl"). Der Name Rijndael ist eine Zusammensetzung aus den ersten beiden Teilen der Nachnamen der Autoren (RIJ + DAE).

Der Algorithmus besitzt eine variable Blockgröße von 128, 192 oder 256 Bit und eine variable Schlüssellänge von 128, 192 oder 256 Bit. Rijndael bietet ein sehr hohes Maß an Sicherheit. Das Verfahren wurde eingehenden kryptoanalytischen Prüfungen unterzogen. Bei Wahl eines entsprechend komplexen Passwortes ist es auch mit größtem Aufwand ohne den jeweiligen Schlüssel nicht möglich die damit codierten Daten zu dechiffrieren. Der Algorithmus ist frei verfügbar und darf ohne Lizenzgebühren eingesetzt oder in Soft- bzw. Hardware implementiert werden. AES ist in den USA für staatliche Dokumente mit höchster Geheimhaltungsstufe zugelassen.

Inhaltsverzeichnis

- 1 Entstehung
  - 1.1 Auswahl eines DES Nachfolgers
- 2 Arbeitsweise
  - 2.1 S-Box
  - 2.2 Ablauf
  - 2.3 Schlüsselexpansion
  - 2.4 KeyAddition
  - 2.5 Substitution
  - 2.6 ShiftRow
  - 2.7 MixColumn
  - 2.8 Entschlüsselung
- 3 Anwendung
- 4 Literatur
- 5 Weblinks

Entstehung

Bisher war der Data Encryption Standard (DES) der am häufigsten genutzte symmetrische Algorithmus zur Verschlüsselung von Daten. Trotzdem wurde er oft stark kritisiert. Da er lange Zeit nicht vollständig veröffentlicht war, wurden sogar Hintertüren der amerikanischen National Security Agency (NSA) vermutet, die allerdings nie gefunden wurden. Zweifel an der Sicherheit von DES waren jedoch begründet (schließlich benutzt DES nur einen 56 Bit langen Schlüssel) und wurden durch die Electronic Frontier Foundation (EFF) bestätigt, die 1998 eine Maschine zur Entschlüsselung von DES mittels Brute-Force-Verfahren bauten. 3DES bot sich als eine vorübergehende Lösung an, ist jedoch recht langsam und die verwendete Schlüssellänge von effektiven 112 Bit ist ein potenzielles Sicherheitsrisiko. Es musste also ein neuer Verschlüsselungsstandard entwickelt werden, der nicht die Fehler seiner Vorgänger besitzt.

Auswahl eines DES Nachfolgers

Das US-amerikanische National Institute of Standards and Technology (NIST) hatte Anfang 1997 zu einem offenen Wettbewerb aufgerufen, dessen Sieger als Advanced Encryption Standard (AES) festgelegt werden sollte. Dabei wurden folgende Kriterien aufgestellt, die von den Algorithmen zu erfüllen sind:

- AES muss ein symmetrischer Algorithmus sein, und zwar eine Blockchiffre.

- AES muss mindestens 128 Bit lange Blöcke verwenden und Schlüssel von 128, 192 und 256 Bit Länge einsetzen können.
- AES soll gleichermaßen leicht in Hard- und Software zu implementieren sein.
- AES soll in Hardware wie Software eine überdurchschnittliche Performance haben.
- AES soll allen bekannten Methoden der Kryptoanalyse (die Kunst, einen Geheimtext ohne Kenntnis des Schlüssels zu dechiffrieren) widerstehen können, insbesondere Power- und Timing-Attacken.
- Speziell für den Einsatz in Smartcards sollen geringe Ressourcen erforderlich sein (kurze Codelänge, niedriger Speicherbedarf).
- Der Algorithmus muss frei von patentrechtlichen Ansprüchen sein und darf von jedermann unentgeltlich genutzt werden.

Im August 1998 gingen schließlich 15 Algorithmen beim NIST ein, die öffentlich diskutiert und auf die Erfüllung der genannten Kriterien geprüft wurden. Die engere Wahl war im April 1999 beendet und die fünf besten Kandidaten (MARS, RC6, Rijndael, Serpent, Twofish) kamen in die nächste Runde.

Alle fünf Kandidaten erfüllen die oben genannten Forderungen. Daher wurden weitere Kriterien hinzugezogen. Es folgte eine Überprüfung der Algorithmen auf theoretische Schwachstellen, durch die der Algorithmus möglicherweise irgendwann einmal unsicher werden kann. Dies klingt zwar sehr weit hergeholt, ist aber notwendig. Denn leider kann heute nicht gesagt werden, wie sich der Technologie-Fortschritt in den nächsten Jahren entwickelt. Vorgehensweisen, die heute als unmöglich erklärt sind, können in einigen Jahren schon alltäglich sein. Ein solches Risiko darf nicht eingegangen werden.

Eindeutiger war jedoch die Staffelung der Kandidaten nach Ressourcenverbrauch und Performance. Denn nur der Rijndael-Algorithmus ist als Hardware- und Software-Implementierung überdurchschnittlich schnell. Andere Kandidaten haben jeweils in unterschiedlichen Bereichen kleinere Schwächen.

Im Mai 2000 wurden die Analysen und öffentlichen Diskussionen abgeschlossen und am 2. Oktober 2000 der Sieger schließlich bekannt gegeben: Der belgische Algorithmus Rijndael wird neuer Standard. Sicherlich entspricht es nicht der üblichen Sicherheitspolitik in den USA, dass man sich auf einen europäischen Algorithmus berufen soll. Aber Rijndael hat insbesondere durch seine Einfachheit (die Referenz-Implementierung umfasst weniger als 500 Zeilen C-Code) und Performance überzeugt.

Der Auswahlprozess faszinierte weltweit viele Kryptographen, insbesondere durch seine offene Gestaltung. Bis heute wird dieser Wettbewerb als sehr vorbildlich dargestellt.

Arbeitsweise

AES (im Folgenden ist mit "AES" der Algorithmus Rijndael gemeint) ist, wie bereits erwähnt, eine Blockchiffre, dessen Blocklänge und Schlüssellänge unabhängig voneinander die Werte 128, 192 oder 256 Bits erhalten kann. Jeder Block wird zunächst in eine zweidimensionale Tabelle mit vier Zeilen geschrieben, dessen Zellen ein Byte groß sind. Die Anzahl der Spalten variiert somit je nach Blockgröße von 4 (128 Bits) bis 8 (256 Bits). Jeder Block wird nun nacheinander bestimmten Transformationen unterzogen. Aber anstatt jeden Block einmal mit dem Schlüssel zu verschlüsseln, wendet AES verschiedene Teile des Schlüssels nacheinander auf den Klartext-Block an. Die Anzahl *r* dieser Runden variiert und ist von der Schlüssellänge *k* und Blockgröße *b* abhängig:

Je nach Blocklänge b und Schlüssellänge k wird die Anzahl der Runden bestimmt (10, 12 oder 14)

r	b=128	b=192	b=256
k=128	10	12	14
k=192	12	12	14
k=256	14	14	14

S-Box

Eine Substitutionsbox (S-Box) dient als Basis für eine monoalphabetische Verschlüsselung. Sie ist meist als Array

implementiert und gibt an, welches Byte wie getauscht wird. Die S-Box in AES basiert auf einem mathematischen Zusammenhang und ist somit fest im Algorithmus implementiert. Doch dies ist kein Schwachpunkt, da die S-Box lediglich zur Vermischung der Bytes in Kombination mit weiteren Operationen und dem Schlüssel genutzt wird.

Ablauf

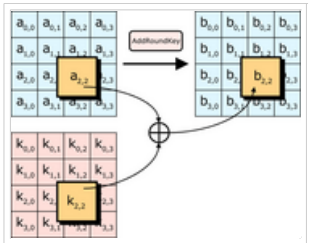
- Schlüsselexpansion
- Vorrunde
  - KeyAddition ()
- Verschlüsselungsrunden (wiederhole solange runde<r)
  - Substitution()
  - ShiftRow()
  - MixColumn()
  - KeyAddition()
- Schlussrunde
  - Substitution()
  - ShiftRow()
  - KeyAddition()

Schlüsselexpansion

Zunächst muss der Schlüssel in $r + 1$ Teilschlüssel (auch Rundenschlüssel genannt) aufgeteilt werden. Die Rundenschlüssel müssen die gleiche Länge wie die Blöcke erhalten. Somit muss der Benutzerschlüssel auf die Länge $b * (r + 1)$ expandiert werden. Die Schlüssel werden wieder in zweidimensionalen Tabellen mit vier Zeilen und Zellen der Größe 1 Byte gebildet. Die ersten Spalten der Tabelle werden mit dem Benutzerschlüssel gefüllt. Die weiteren Spalten werden wie folgt rekursiv berechnet: Um die Werte für die Zellen in der nächsten Spalte zu erhalten, wird zunächst das Byte, welches sich in der letzten (je nach Blockgröße: vierten, sechsten oder achten) Spalte befindet und drei Zeilen zurückliegt, durch die S-Box verschlüsselt und anschließend mit dem um eine Schlüssellänge zurückliegendem Byte XOR verknüpft. Befindet sich das zu berechnende Byte an einer Position, die ein ganzzahliger Teiler der Schlüssellänge ist, so wird das berechnete Byte zusätzlich mit einem Eintrag aus der rcon-Tabelle XOR verknüpft. Hierfür wird als Index eine fortlaufende Nummer verwendet. Die rcon-Tabelle ist ähnlich wie die S-Box eine Tabelle in Form eines Arrays, das konstante Werte enthält die auf einem mathematischen Zusammenhang beruhen. Jedes weitere Byte (das sich nicht in der ersten Spalte befindet) wird aus einer XOR-Verknüpfung des vorherigen Bytes (w_{i-1}) mit dem Byte einer Schlüssellänge vorher ($w_{i-k/32}$) gebildet.

KeyAddition

In der Vorrunde und nach jeder weiteren Verschlüsselungsrunde wird die KeyAddition ausgeführt. Hierbei wird eine bitweise XOR-Verknüpfung zwischen dem Block und dem aktuellen Rundenschlüssel vorgenommen. Dies ist die einzige Funktion in AES, die den Algorithmus vom Benutzerschlüssel abhängig macht.



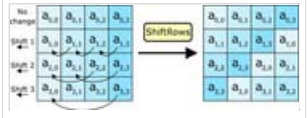
Bitweise XOR-Verknüpfung zwischen dem Block und dem aktuellen Rundenschlüssel

Substitution

Im ersten Schritt jeder Runde wird für jedes Byte im Block ein Äquivalent in der S-Box gesucht. Somit werden die Daten monoalphabetisch verschlüsselt.

ShiftRow

Wie oben erwähnt, liegt ein Block in Form einer zweidimensionalen Tabelle mit vier Zeilen vor. In diesem Schritt werden die Zeilen um eine bestimmte Anzahl von Spalten nach links verschoben. Überlaufende Zellen werden von rechts fortgesetzt. Die Anzahl der Verschiebungen ist zeilen- und blocklängenabhängig:



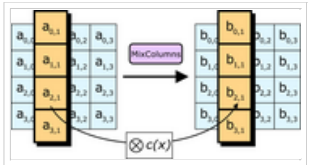
Zeilen werden um eine bestimmte Anzahl von Spalten nach links verschoben

Je nach Blocklänge b und Zeile in der Datentabelle wird die Zeile um 1 bis 4 Spalten verschoben

r	b=128	b=192	b=256
Zeile 0	0	0	0
Zeile 1	1	1	1
Zeile 2	2	2	3
Zeile 3	3	3	4

MixColumn

Schließlich werden die Spalten vermischt. Es wird zunächst jede Zelle einer Spalte mit einer Konstanten multipliziert und anschließend die Ergebnisse XOR verknüpft. Hinter dieser Vorgehensweise steckt ein komplizierter mathematischer Zusammenhang, der hier nicht näher erläutert wird. Die Konstante wird folgendermaßen bestimmt:



Die Spalten werden vermischt

Zeile 1: 2
Zeile 2: 3
Zeile 3: 1
Zeile 4: 1

Entschlüsselung

Bei der Entschlüsselung von Daten wird genau rückwärts vorgegangen. Die Daten werden zunächst wieder in zweidimensionale Tabellen gelesen und die Rundenschlüssel generiert. Allerdings wird nun mit der Schlussrunde angefangen und alle Funktionen in jeder Runde in der umgekehrten Reihenfolge aufgerufen. Durch die vielen XOR-Verknüpfungen unterscheiden sich die meisten Funktionen zum Entschlüsseln nicht von denen zum Verschlüsseln. Jedoch muss eine andere S-Box genutzt werden (die sich aus der original S-Box berechnen lässt) und die Zeilenverschiebungen erfolgen in die andere Richtung.

Anwendung

AES wird u. a. vom Verschlüsselungsstandard 802.11i für Wireless LAN und seinem Wi-Fi-Äquivalent WPA2 sowie bei SSH und bei IPsec genutzt. Außerdem wird der Algorithmus zur Verschlüsselung diverser komprimierter Dateiarchive verwendet. Des Weiteren nutzt Skype laut eigenen Angaben AES. Das Datenkomprimierungsprogramm 7-Zip verwendet AES zur Verschlüsselung der Archive. In PGP (und natürlich auch GnuPG) findet AES auch einen großen Anwendungsbereich.

Literatur

- Joan Daemen, Vincent Rijmen: *The Design of Rijndael. The Wide Trail Strategy.* ISBN 3540425802 (Englisch)

Weblinks

- http://csrc.nist.gov/CryptoToolkit/aes/ - Offizielle AES-Website des NIST
- http://www.esat.kuleuven.ac.be/~rijmen/rijndael/ - Website vom Rijndael-Autor Vincent Rijmen
- http://www.realtec.de/privat/arbeiten.shtml - Ausführlichere deutsche Erklärung des Algorithmus (PDF)
- http://www.cryptosystem.net/aes/ - Angriffe auf die Sicherheit von AES
- http://www-cse.ucsd.edu/~fritz/rijndael.html - freie JavaScript Implementierung (für die API noch gut zu wissen: CBC ist besser als ECB und hier (http://www.fourmilab.com/onetime/otpjs.html) gibt es eine bessere random()-Funktion)

Siehe auch: Kryptographie

Von "http://de.wikipedia.org/wiki/Advanced_Encryption_Standard"

Kategorie: Verschlüsselungsverfahren

- Diese Seite wurde zuletzt geändert um 16:24, 31. Okt 2005.
- Ihr Inhalt steht unter der GNU-Lizenz für freie Dokumentation