Der Advanced Encryption Standard

4

Der *Advanced Encryption Standard* (AES) ist die heutzutage am meisten genutzte symmetrische Chiffre überhaupt. Die AES-Blockchiffre ist für zahlreiche behördliche und industrielle Anwendungen als Standard vorgeschrieben. Zu den weit verbreiteten Standards, die AES verwenden, gehören u. a. TLS, der Internetsicherheitsstandard IPsec, der WLAN-Verschlüsselungsstandard IEEE 802.11i, das Secure-Shell-Protokoll SSH oder zur Sprachverschlüsselung von Skype. Darüber hinaus gibt es unzählige weitere Sicherheitslösungen, bei denen AES zum Einsatz kommt. Bis heute gibt es keine Angriffe auf AES, die signifikant besser als vollständige Schlüsselsuche sind.

In diesem Kapitel erlernen Sie

- den Auswahlprozess, der zum AES geführt hat,
- die Ver- und Entschlüsselungsfunktion von AES,
- die interne Struktur von AES, namentlich
  - Byte-Substitution-Schicht,
  - Diffusionsschicht,
  - Key-Addition-Schicht,
  - Schlüsselfahrplan,
- die Grundlagen zu endlichen Körpern,
- Implementierungseigenschaften von AES.

4.1 Einführung

1999 gab das amerikanische National Institute of Standards and Technology (NIST) bekannt, dass Data Encryption Standard (DES) nur noch aus Kompatibilitätsgründen für bestehende Systeme genutzt werden und stattdessen Triple-DES (3DES) verwendet werden sollte. Obwohl 3DES auch mit heutiger Technologie Brute-Force-Angriffen widersteht, weist er einige Nachteile auf. Zunächst ist zu beachten, dass 3DES nicht sonderlich

C. Paar, J. Pelzl, *Kryptografie verständlich*, eXamen.press, DOI 10.1007/978-3-662-49297-0_4

effizient in Software ist. DES selbst ist nicht gut geeignet für Softwareimplementierungen und 3DES ist dreimal langsamer als der einfache DES. Ein weiterer Nachteil ist die relative kleine Blockgröße von 64 Bit, die sowohl aus theoretischen Betrachtungen nicht wünschenswert ist, als auch praktische Nachteile hat, beispielsweise wenn man Hash-Funktionen aus Blockchiffren bauen möchte (vgl. Abschn. 11.3.2). Ein weiterer Grund sind zukünftige Angriffe mit Quantencomputern, die in einigen Jahrzehnten Realität werden könnten: Um Blockchiffren resistent gegen Quantencomputer zu machen, sind Schlüssellängen von 256 Bit wünschenswert. All diese Betrachtungen haben das NIST zu dem Schluss gebracht, dass eine vollständig neue Blockchiffre als Nachfolger des DES benötigt wird.

1997 hat das NIST eine Ausschreibung für den neuen AES veröffentlicht. Im Gegensatz zur Entwicklung des DES war die Auswahl des AES-Algorithmus ein öffentlicher Prozess, begleitet durch das NIST. In drei aufeinanderfolgenden AES-Evaluierungsrunden haben das NIST und die internationale wissenschaftliche Gemeinschaft Vor- und Nachteile der eingereichten Chiffren diskutiert und damit die Anzahl der potenziellen Kandidaten reduziert. Im Jahr 2001 hat das NIST schließlich die Blockchiffre *Rijndael* als den neuen AES vorgestellt und in dem Standard FIPS PUB 197 veröffentlicht. Rijndael wurde von zwei jungen belgischen Kryptografen entwickelt.

In der ursprünglichen Ausschreibung waren folgende Anforderungen für alle AES-Kandidaten verpflichtend:

- Blockchiffre mit 128 Bit Blockgröße;
- Unterstützung von drei Schlüssellängen: 128, 192 und 256 Bit;
- hohe Sicherheit relativ zu den anderen eingereichten Algorithmen und
- Effizienz in Soft- und Hardware.

Abb. 4.1 stellt die Ein- und Ausgabeparameter des AES dar. Die Ausschreibung und der nachfolgende Auswahlprozess erfolgten öffentlich. Hier ist eine kompakte Chronologie des AES-Auswahlprozesses :

- Die Notwendigkeit für eine neue Blockchiffre wird am 2. Januar 1997 vom NIST angekündigt.
- Eine formelle Ausschreibung für den AES wurde am 12. September 1997 bekannt gegeben.
- Bis zum 20. August 1998 wurden 15 Kandidaten für den AES von Wissenschaftlern aus aller Welt eingereicht.
- Am 9. August 1999 wurden die fünf finalen Kandidaten bekannt gegeben:
  - *Mars* von IBM,
  - *RC6* von RSA Laboratories,
  - *Rijndael* von Joan Daemen und Vincent Rijmen,
  - *Serpent* von Ross Anderson, Eli Biham und Lars Knudsen,
  - *Twofish* von Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall und Niels Ferguson.

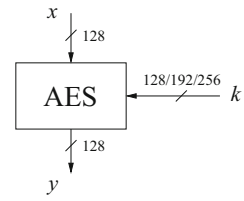

Abb. 4.1 AES-Ein- und -Ausgabeparameter

- Am 2. Oktober 2000 gab das NIST bekannt, dass die Wahl auf Rijndael als AES gefallen ist.
- Am 26. November 2001 wurde der AES formal als US-Standard freigegeben.

Es ist zu erwarten, dass AES in den nächsten Jahrzehnten weiterhin der dominante symmetrische Algorithmus für viele Anwendungen bleibt. Ebenfalls erwähnenswert ist die Tatsache, dass die amerikanische National Security Agency (NSA) im Jahr 2003 bekannt gab, dass es erlaubt ist, vertrauliche Dokumente für die Regierungskommunikation bis zur Stufe SECRET mit AES mit allen Schlüssellängen und bis zur Stufe TOP SECRET mit den Schlüssellängen 192 oder 256 Bit zu verschlüsseln. Vor dieser Bekanntgabe wurden nur geheime Algorithmen für die Verschlüsselung von klassifizierten Dokumenten verwendet.

4.2 Übersicht über den AES-Algorithmus

Die AES-Chiffre ist fast identisch zu der Blockchiffre Rijndael. Die Blockgröße und Schlüssellänge von Rijndael variiert zwischen 128, 192 und 256 Bit. Der AES-Standard erlaubt jedoch nur eine Blockgröße von 128 Bit. Daher ist nur Rijndael mit eine Blockgröße von 128 Bit als AES-Algorithmus bekannt. Im weiteren Verlauf dieses Kapitels werden wir nur die Standardversion des Rijndael mit einer Blockgröße von 128 Bit besprechen.

Wie bereits zuvor erwähnt, musste Rijndael laut NIST-Anforderung drei Schlüssellängen unterstützen. Die Anzahl der internen Runden der Chiffre ist, wie in Tab. 4.1 zu sehen, eine Funktion der Schlüssellänge.

Im Gegensatz zum DES hat der AES keine Feistel-Struktur. Feistel-Netzwerke verschlüsseln pro Iteration nicht den gesamten Block. Beim DES beispielsweise werden $64/2 = 32$ Bits in einer Runde verschlüsselt. Im Gegensatz hierzu verschlüsselt AES in jeder Runde alle 128 Bits. Dies ist einer der Gründe, warum der AES vergleichsweise wenige Runden hat.

Tab. 4.1 Schlüssellänge und Anzahl der Runden für AES

Schlüssellänge	# Runden $= n_r$
128 Bit	10
192 Bit	12
256 Bit	14

AES besteht aus sog. *Schichten* („layer“). Jede Schicht manipuliert alle 128 Bits des Datenpfads. Den Datenpfad nennt man auch den *Zustand* des Algorithmus. Es gibt nur drei verschiedene Arten von Schichten. Mit Ausnahme der letzten Runde besteht jede Runde aus allen drei Schichten, wie in Abb. 4.2 dargestellt: Der Klartext wird hierbei mit x bezeichnet, das Chiffrat mit y und die Anzahl der Runden mit n_r, wobei $n_r = 10, 12, 14$. Jedoch wird in der letzten Runden n_r nicht die MixColumn-Transformation verwendet, wodurch die AES-Ver- und -Entschlüsselung symmetrisch aufgebaut sind.

Nachfolgend werden die Schichten kurz beschrieben:

Key-Addition-Schicht Ein 128-Bit-Rundenschlüssel (auch Unterschlüssel genannt), der von dem Hauptschlüssel im Schlüsselfahrplan abgeleitet wird, wird auf den Zustand per XOR addiert.

Byte-Substitution-Schicht (S-Box) Jedes Byte des Zustands wird über eine nichtlineare Transformation durch ein anderes Byte ersetzt. Dies erfolgt mit einer S-Box mit speziellen mathematischen Eigenschaften. Die S-Boxen sind die Konfusionselemente des AES.

Diffusionsschicht Diese Schicht erzeugt *Diffusion* über alle Zustandbits. Die Schicht besteht aus zwei Unterschichten, die beide lineare Operationen durchführen:

- Die *ShiftRows*-Operation permutiert die Daten byteweise.
- Die *MixColumn*-Operation ist eine Matrixmultiplikation, die Blöcke von jeweils vier Bytes verwürfelt.

Analog zum DES berechnet der Schlüsselfahrplan die Rundenschlüssel $(k_0, k_1, \ldots, k_{n_r})$ aus dem AES-Hauptschlüssel.

Bevor wir die internen Funktionen der Schichten genauer in Abschn. 4.4 untersuchen, müssen wir ein neues mathematisches Konzept, nämlich das der *endlichen Körper*, einführen.

4.3 Eine kurze Einführung in endliche Körper

In den meisten Schichten erfordert AES das Rechnen in endlichen Körpern, insbesondere bei der S-Box und der MixColumn-Schicht. Für ein besseres Verständnis der AES-Interna ist daher eine Einführung in endliche Körper notwendig, bevor wir mit der eigentlichen Chiffre in Abschn. 4.4 fortfahren. Für ein rudimentäres Verständnis von AES ist das Wissen über endliche Körper jedoch nicht zwingend erforderlich und dieser Abschnitt kann in dem Fall übersprungen werden.