AES

Die AES-Verschlüsselung ist ein weit verbreiteter Algorithmus oder eine sogenannte Blockchiffre, um Wifi-, Browser-Verbindungen und Daten zu verschlüsseln. In diesem Ratgeber-Artikel versuchen wir, das mathematisch komplexe Thema AES-Verschlüsselung möglichst umfassend, aber auch **so einfach darzustellen, dass jede und jeder es verstehen kann**.

Was ist eine AES-Verschlüsselung?

AES steht für Advanced Encryption Standard. Die AES-Verschlüsselung ist **ein gängiges Verfahren oder eine Blockchiffre zur Verschlüsselung von Dokumenten, Verbindungen und Servern**. Es handelt sich dabei um eine symmetrische Verschlüsselung: d.h. die Ver- und Entschlüsselung erfolgt mit ein und demselben Schlüssel. AES ermöglicht dabei unterschiedliche Längen der verwendeten Schlüssel, die in der dabei verwendeten Anzahl Bits in einem Kürzel dargestellt werden: AES-128, AES-192 und AES-256.

Anwendung von AES

AES ist ein schwer zu knackendes Verschlüsselungsverfahren, das vom U.S. National Institute of Standards and Technology (NIST) im Jahr 2001 als Standard etabliert wurde. Er wird **weltweit in Software und Hardware eingesetzt, um sensible Daten zu verschlüsseln** und ist für die heutige Cybersicherheit und den Schutz elektronischer Daten unerlässlich. AES kann folgende Anwendungen verschlüsseln:

- 

  Daten

- 

  Wi-Fi

- 

Browser

- **Daten-Verschlüsselung**: AES dient oft zur sicheren Verschlüsselung von sogenannten Data-at-Rest – also Daten, die physisch auf einem Server, einer Festplatte oder in einer Cloud liegen.
- **Wifi-Verschlüsselung**: AES ist ein sicheres Verfahren, um ein drahtloses Netzwerk zu verschlüsseln und zu sichern. Es ist in den WPA2- und WPA3-Standards enthalten.
- **Browser-Verschlüsselung**: AES ist eines der Verschlüsselungsverfahren, das im TLS-Protokoll zur Anwendung kommt. TLS sorgt für das sichere Vorhängeschloss-Icon, das im Browser eine sichere Verbindung anzeigt.

Wie funktioniert AES?

Eines sollten Sie von vornherein wissen: Ohne das richtige mathematische Hintergrundwissen ist der AES-Verschlüsselungsalgorithmus schwer zu verstehen. Wir werden aber versuchen, die **Funktionsweise des AES so stark wie möglich zu vereinfachen**.

Substitutions-Permutations-Netzwerk

Die AES-Blockchiffre schützt die Informationen, die sie verschlüsselt, **indem sie sie in Stücke zerteilt und in ein scheinbar zufälliges Durcheinander verwandelt**. Dazu nutzt AES ein für Blockchiffren entworfenes Designprinzip – das sogenannte Substitutions-Permutations-Netzwerk. Dieses besteht aus einer Anzahl von Runden gleichen Aufbaus, die zwischen den Verfahren Substitution und Permutation wechseln.

- Bei der **Substitution** werden Klartextbuchstaben oder -buchstabenketten durch Buchstaben, Zahlen oder Symbole ersetzt.
- Bei der **Permutation** werden die Buchstaben der Klartextnachricht verwendet, aber in einer anderen Reihenfolge angeordnet.

Die 4 Schritte jeder Verschlüsselungs-Runde

Die Verschlüsselung erfolgt in 10 (128 Bit), 12 (192 Bit) oder 14 Runden (256 Bit). Eine Runde setzt sich dabei **aus mehreren mathematischen Schritten zusammen**, die umkehrbar sind, um neben der sicheren Ver- auch die Entschlüsselung zu garantieren.

- **Sub Byte:** In diesem Schritt wird jedes Byte mit einer Substitutionsbox (S-Box) verschlüsselt. Die S-Box gibt dabei eine Regel an, wie ein Byte eines Blockes durch einen anderen Wert zu ersetzen ist. Dadurch werden die Bytes vermischt.
- **Shift Row:** Nun verschiebt AES die Bytes in den Blöcken zeilenweise um eine bestimmte Anzahl von Spalten nach links.
- **Mix Column:** In diesem Schritt geht es nun darum, die Spalten zu vermischen. Hierfür wird jede Spalte mit einer bestimmten Matrix multipliziert.
- **Key Addition:** Hier wird nun jeder Block mit dem aktuellen Rundenschlüssel XOR verknüpft.

AES-128, AES-192, AES-256: Was ist der Unterschied?

Der Unterschied besteht **in der Länge der jeweiligen Schlüssel**: 128 Bit, 192 Bit oder 256 Bit. Je länger der Schlüssel, desto höher ist die Sicherheit. Dabei verschlüsselt und entschlüsselt AES immer in Blöcken von 128 Bit – unabhängig von der Länge des verwendeten Schlüssels. Je nach Schlüssellänge ergeben sich so 10 Verschlüsselungs-Runden für 128 Bit, 12 für 192 Bit und 14 für 256 Bit.

Entwicklung des Advanced Encryption Standards

AES wurde ursprünglich von den **zwei belgischen Programmierern Joan Daemen und Vincent Rijmen** entwickelt und nach ihren Nachnamen Rijndael genannt. Im Oktober 2000 kündigte das amerikanische National Institute of Standards and Technology (NIST) an, dass es den Advanced Encryption Standard (AES) – eine Variante des ursprünglichen Rijndael – als neuen Standard anerkennt und ab sofort den alten und unsicher gewordenen Data Encryption Standard (DES) ersetzt.

Die AES-Verschlüsselung ist ein gängiges Verfahren zur Verschlüsselung von Dokumenten und Co.

Wie sicher ist AES?

AES erweist sich auch mehr als 20 Jahre nach seiner Entwicklung und Festlegung als weltweiter Standard **als sehr sicher**. Es sind bisher keine nennenswerten Schwächen bekannt geworden. Selbst wenn es theoretisch möglich ist, AES zu knacken, ist der Aufwand dafür unbeschreiblich groß. AES wurde daher noch nie geknackt und ist entgegen allen Behauptungen auch sicher gegen Brute-Force-Angriffe. Daher nutzt Skribble AES zur Verschlüsselung aller Kundendokumente.

Längere Schlüssel für zusätzliche Sicherheit

Die Sicherheit von AES ist **unter anderem auch von der Schlüssellänge abhängig**. Schon bei einer Schlüssellänge von 128 Bit ist die vollständige Schlüsselsuche erfolglos. Es ist jedoch davon auszugehen, dass die Rechenleistung neuerer Computer schnell voranschreitet und die

Schlüssellänge zum Knackpunkt wird. Es empfiehlt sich daher schon heute, eine Schlüssellänge von 256 Bit zu wählen, um genug Sicherheitspuffer für die Zukunft zu haben.

Wie lange bleibt AES noch sicher?

Mit zunehmender Rechnergeschwindigkeit und der rasanten technologischen Entwicklung wird trotz der enormen Sicherheit irgendwann der Zeitpunkt kommen, an dem AES abgelöst wird. Wie lange AES noch sicher verwendet werden kann, **ist nicht mit Bestimmtheit zu sagen**. Sicher noch für eine ganze Weile.

Alternativen zu AES

Alternative 1: Rivest-Shamir-Adleman (RSA)

Der Rivest-Shamir-Adleman-Verschlüsselungsalgorithmus (RSA) ist ein asymmetrischer Verschlüsselungsalgorithmus, der für viele Produkte und Dienstleistungen verwendet wird. Im Gegensatz zu AES **arbeitet er mit zwei Schlüsselpaaren** – einem privaten und einem öffentlichen Schlüssel.

Alternative 2: Triple DES

Bei Triple DES handelt es sich um eine Anwendung des alten DES-Algorithmus (Data Encryption Standard), bei der drei Durchläufe anstelle eines einzigen verwendet werden. Triple DES bietet eine viel stärkere Verschlüsselung als der normale DES, ist aber **weniger sicher als der Advanced Encryption Standard (AES) und wird heute als unsicher betrachtet**.

Alternative 3: Twofish

Twofish ist **ähnlich wie AES eine symmetrische Blockchiffre** mit einer Blockgröße von 128 Bit und Schlüsselgrößen von bis zu 256 Bit. Er war einer der fünf Finalisten des Advanced-Encryption-Standard-Wettbewerbs, wurde am Ende aber nicht für die Standardisierung ausgewählt.

AES-Verschlüsselung: Datensicherheit auf höchstem Niveau

Die AES-Verschüsselung ist ein wichtiger Standard für die symmetrische Verschlüsselung von Klartextdaten, der auf der ganzen Welt **für eine Vielzahl von Anwendungen wie sichere Wifi- und Browserverbindungen und Daten verwendet wird**. AES gibt es in drei verschiedenen Schlüssellängen: 128 Bit, 192 Bit und 256 Bit. Je länger der Schlüssel, desto sicherer ist die Verschlüsselung.