

Symmetrische Verschlüsselung

Weitere Bezeichnungen: Symmetrische Chiffrierung

Rubrik: Sicherheit

Die symmetrische Verschlüsselung ist ein kryptografisches Verfahren, bei dem derselbe geheime Schlüssel sowohl zum Verschlüsseln als auch zum Entschlüsseln von Daten verwendet wird. Sie gehört zu den grundlegenden Methoden der modernen Kryptografie und dient dazu, vertrauliche Informationen vor unbefugtem Zugriff zu schützen. Symmetrische Verschlüsselungsverfahren werden unter anderem bei der Speicherung von Daten, der Absicherung von Netzwerkverbindungen und der verschlüsselten Kommunikation eingesetzt.

Bei der symmetrischen Verschlüsselung werden die ursprünglichen Daten, der sogenannte Klartext, mithilfe eines Verschlüsselungsalgorithmus und eines geheimen Schlüssels in einen nicht unmittelbar lesbaren Geheimtext umgewandelt. Um die Informationen wiederherzustellen, benötigt der Empfänger denselben Schlüssel. Dieser muss deshalb vor unbefugtem Zugriff geschützt und bei einer Kommunikation zwischen mehreren Teilnehmern auf sichere Weise ausgetauscht werden.

Grundsätzlich unterscheidet man zwischen Blockchiffren und Stromchiffren. Blockchiffren verarbeiten Daten in Blöcken fester Größe. Ein bekanntes Beispiel ist der Advanced Encryption Standard (AES), der mit einer Blockgröße von 128 Bit arbeitet. Stromchiffren erzeugen dagegen einen schlüsselabhängigen Datenstrom, der mit den zu verschlüsselnden Informationen kombiniert wird. Ein verbreitetes Beispiel ist ChaCha20.

Zu den bekanntesten symmetrischen Verschlüsselungsalgorithmen gehören AES, DES, Triple DES, Blowfish und Twofish. Während AES heute zu den wichtigsten modernen Verfahren zählt, gelten DES und Triple DES aufgrund ihrer technischen Einschränkungen als veraltet. Auch Blowfish wird wegen seiner vergleichsweise kleinen Blockgröße von 64 Bit für neue Anwendungen nicht mehr empfohlen.

Ein wesentlicher Vorteil der symmetrischen Verschlüsselung ist ihre hohe Verarbeitungsgeschwindigkeit. Im Vergleich zu asymmetrischen Verschlüsselungsverfahren benötigt sie bei großen Datenmengen in der Regel deutlich weniger Rechenleistung. Deshalb eignet sie sich besonders für die Verschlüsselung von Festplatten, SSDs, Dateien und umfangreichen Datenübertragungen. Moderne Prozessoren besitzen häufig spezielle Befehlserweiterungen, mit denen beispielsweise AES-Berechnungen beschleunigt werden können.

Eine Herausforderung ist die sichere Schlüsselverteilung. Da alle berechtigten Teilnehmer den

geheimen Schlüssel kennen müssen, darf dieser nicht über einen ungeschützten Kommunikationsweg übertragen werden. In vielen modernen Sicherheitsprotokollen werden deshalb asymmetrische Verfahren zum Aufbau eines gemeinsamen Geheimnisses eingesetzt. Aus diesem werden anschließend symmetrische Sitzungsschlüssel abgeleitet, mit denen die eigentlichen Nutzdaten effizient verschlüsselt werden.

Die symmetrische Verschlüsselung ist ein zentraler Bestandteil moderner IT-Sicherheit. Sie kommt beispielsweise bei HTTPS-Verbindungen, WLAN-Verschlüsselung, VPN-Verbindungen und der Festplattenverschlüsselung zum Einsatz. Ihre Sicherheit hängt insbesondere von einem geeigneten Algorithmus, ausreichend starken Schlüsseln, der korrekten Verwendung von Betriebsmodi und einer zuverlässigen Schlüsselverwaltung ab.

Weiterführende Informationen

AES, ChaCha20, Twofish, Blowfish, DES