

DES

Weitere Bezeichnungen: Data Encryption Standard

Rubrik: Kryptografie

DES (Data Encryption Standard) ist ein symmetrischer Verschlüsselungsalgorithmus, der 1977 als offizieller US-amerikanischer Verschlüsselungsstandard veröffentlicht wurde. Das Verfahren wurde auf Grundlage eines von IBM entwickelten Algorithmus namens Lucifer konzipiert und unter Beteiligung der US-amerikanischen National Security Agency (NSA) weiterentwickelt. DES gehörte über viele Jahre zu den wichtigsten Verfahren zum Schutz digitaler Informationen und hatte einen erheblichen Einfluss auf die Entwicklung der modernen Kryptografie.

DES ist eine sogenannte Blockchiffre. Der Algorithmus verarbeitet Daten in Blöcken mit einer festen Größe von 64 Bit. Zur Verschlüsselung verwendet er einen Schlüssel mit einer Gesamtlänge von 64 Bit, von denen jedoch nur 56 Bit tatsächlich als Schlüsselmaterial dienen. Die übrigen acht Bits sind für Paritätsinformationen vorgesehen. Die vergleichsweise geringe effektive Schlüssellänge stellt aus heutiger Sicht die größte Sicherheitsschwäche des Verfahrens dar.

Der Verschlüsselungsvorgang basiert auf einem Feistel-Netzwerk mit insgesamt 16 Runden. Zu Beginn wird der Datenblock einer festgelegten Anfangspermutation unterzogen und anschließend in zwei Hälften aufgeteilt. In jeder Runde werden die Daten mithilfe einer Rundenfunktion, eines abgeleiteten Rundenschlüssels und einer XOR-Verknüpfung verarbeitet. Nach Abschluss der 16 Runden wird eine abschließende Permutation durchgeführt, wodurch der verschlüsselte Datenblock entsteht.

Eine wichtige Eigenschaft von DES ist, dass zur Verschlüsselung und Entschlüsselung derselbe geheime Schlüssel verwendet wird. Die Entschlüsselung erfolgt mit derselben grundlegenden Feistel-Struktur, wobei die Rundenschlüssel in umgekehrter Reihenfolge eingesetzt werden. Damit gehört DES zur Gruppe der symmetrischen Verschlüsselungsverfahren.

DES wurde über viele Jahre in Computersystemen, Kommunikationsnetzen und insbesondere im Finanzwesen eingesetzt. Mit zunehmender Rechenleistung erwies sich die Schlüssellänge von 56 Bit jedoch als unzureichend. Im Jahr 1998 demonstrierte die Electronic Frontier Foundation (EFF) mit einer speziell entwickelten Maschine, dass ein DES-Schlüssel durch systematisches Ausprobieren innerhalb weniger Tage ermittelt werden konnte. Dieser Angriff verdeutlichte die praktische Verwundbarkeit des Algorithmus gegenüber Brute-Force-Angriffen.

Als Übergangslösung wurde Triple DES (3DES) verwendet. Bei diesem Verfahren wird der DES-Algorithmus mehrfach hintereinander angewendet, um die Sicherheit gegenüber einfachem DES zu erhöhen. Allerdings besitzt auch Triple DES technische Einschränkungen, insbesondere durch seine Blockgröße von 64 Bit und die vergleichsweise geringe Verarbeitungsgeschwindigkeit. Für neue Anwendungen wird deshalb weder DES noch Triple

DES empfohlen.

Der moderne Nachfolger von DES ist der Advanced Encryption Standard (AES), der im Jahr 2001 als US-amerikanischer Standard veröffentlicht wurde. AES verwendet eine Blockgröße von 128 Bit und unterstützt Schlüssellängen von 128, 192 und 256 Bit. DES besitzt heute vor allem historische und wissenschaftliche Bedeutung, da sein Aufbau und seine Sicherheitsanalyse die Entwicklung zahlreicher späterer Verschlüsselungsalgorithmen beeinflusst haben.

Weiterführende Informationen

Triple DES, AES, Symmetrische Verschlüsselung, Blockchiffre, Feistel-Netzwerk, Brute-Force-Angriff, Lucifer