

Feistel-Netzwerk

Weitere Bezeichnungen: Feistel-Struktur

Rubrik: Sicherheit

Ein Feistel-Netzwerk ist eine kryptografische Struktur, die beim Aufbau symmetrischer Verschlüsselungsalgorithmen verwendet wird. Sie wurde nach dem deutsch-amerikanischen Kryptografen Horst Feistel benannt, der in den 1970er-Jahren maßgeblich an der Entwicklung entsprechender Verschlüsselungsverfahren beteiligt war. Feistel-Netzwerke bilden die Grundlage zahlreicher bekannter Blockchiffren, darunter DES, Blowfish und Twofish.

Das grundlegende Prinzip besteht darin, einen Datenblock in zwei Teilblöcke aufzuteilen. Diese werden anschließend in mehreren aufeinanderfolgenden Verarbeitungsschritten, den sogenannten Runden, miteinander verknüpft. Ziel ist es, die ursprünglichen Daten so zu verändern, dass ohne den passenden geheimen Schlüssel keine einfache Rekonstruktion möglich ist.

In einer klassischen Feistel-Runde wird einer der beiden Teilblöcke mithilfe einer Rundenfunktion verarbeitet. Dabei fließt normalerweise ein aus dem geheimen Schlüssel abgeleiteter Rundenschlüssel ein. Das Ergebnis wird durch eine XOR-Verknüpfung mit dem anderen Teilblock kombiniert. Anschließend werden die Rollen der beiden Teilblöcke für die nächste Runde vertauscht. Durch die wiederholte Anwendung dieses Verfahrens entsteht eine zunehmend komplexe Abhängigkeit zwischen den Eingabedaten und dem Schlüssel.

Eine wichtige Eigenschaft des Feistel-Netzwerks ist seine Umkehrbarkeit. Die Rundenfunktion selbst muss nicht umkehrbar sein, damit sich der gesamte Verschlüsselungsvorgang rückgängig machen lässt. Bei der Entschlüsselung werden die Rundenschlüssel in umgekehrter Reihenfolge verwendet. Dadurch können Verschlüsselung und Entschlüsselung mit einer weitgehend identischen Struktur durchgeführt werden.

Die Sicherheit eines Feistel-basierten Verschlüsselungsalgorithmus hängt wesentlich von der Gestaltung der Rundenfunktion, der Anzahl der Runden und der Erzeugung der Rundenschlüssel ab. Eine sorgfältig entwickelte Rundenfunktion soll dafür sorgen, dass sich Veränderungen einzelner Eingabebits auf viele Bits des verschlüsselten Datenblocks auswirken. Dieser Effekt wird als Lawineneffekt bezeichnet.

Ein bekanntes Beispiel ist der Data Encryption Standard (DES), der ein Feistel-Netzwerk mit 16 Runden verwendet. Auch Blowfish arbeitet mit 16 Feistel-Runden, während Twofish eine modifizierte Feistel-Struktur mit ebenfalls 16 Runden nutzt. Die Algorithmen unterscheiden sich jedoch deutlich hinsichtlich ihrer Rundenfunktionen, Schlüssellängen und weiteren technischen Eigenschaften.

Feistel-Netzwerke gehören zu den grundlegenden Konstruktionsprinzipien der modernen

Kryptografie. Sie ermöglichen den systematischen Aufbau umkehrbarer Blockchiffren und werden bis heute in der Entwicklung und Analyse kryptografischer Verfahren untersucht. Nicht jede Blockchiffre basiert allerdings auf einem Feistel-Netzwerk: Der weitverbreitete Verschlüsselungsstandard AES verwendet beispielsweise ein anderes Konstruktionsprinzip, das als Substitutions-Permutations-Netzwerk bezeichnet wird.

Weiterführende Informationen

Blockchiffre, Symmetrische Verschlüsselung, Blowfish, Twofish, DES, Rundenfunktion, XOR, Lawineneffekt