

Blowfish ist ein symmetrisches Blockverschlüsselungsverfahren von Bruce Schneier.

Blowfish ist ein symmetrischer Verschlüsselungsalgorithmus, der 1993 vom US-amerikanischen Kryptografen Bruce Schneier entwickelt wurde. Er dient dazu, digitale Informationen vor unbefugtem Zugriff zu schützen. Blowfish wurde als frei nutzbare Alternative zu damals verbreiteten Verschlüsselungsverfahren wie DES (Data Encryption Standard) konzipiert und fand insbesondere in Sicherheitssoftware und verschiedenen Anwendungen zur Datenverschlüsselung Verwendung.

Der Algorithmus gehört zu den sogenannten Blockchiffren. Dabei werden die zu verschlüsselnden Daten in Blöcke fester Größe aufgeteilt und mithilfe eines geheimen Schlüssels verarbeitet. Blowfish verwendet eine Blockgröße von 64 Bit und unterstützt Schlüssellängen zwischen 32 und 448 Bit. Bei der Verschlüsselung und Entschlüsselung wird derselbe geheime Schlüssel verwendet, weshalb Blowfish zu den symmetrischen Verschlüsselungsverfahren zählt.

Blowfish basiert auf einem Feistel-Netzwerk mit insgesamt 16 Verschlüsselungsrunden. Innerhalb dieser Runden werden die Daten durch mathematische Operationen und schlüsselabhängige Ersetzungstabellen verändert. Zu den wichtigsten Bestandteilen gehören sogenannte S-Boxen und ein P-Array. Diese Strukturen werden während der Schlüsselinitialisierung aus dem verwendeten Schlüssel abgeleitet.

Eine Besonderheit von Blowfish ist die vergleichsweise aufwendige Schlüsselvorbereitung. Während die eigentliche Verschlüsselung auf vielen Prozessoren effizient durchgeführt werden kann, benötigt die Initialisierung eines neuen Schlüssels zusätzliche Rechenzeit. Der Algorithmus eignet sich deshalb besonders für Anwendungen, bei denen derselbe Schlüssel über längere Zeit verwendet wird.

Blowfish wurde unter anderem in Verschlüsselungsprogrammen und älteren Sicherheitsanwendungen eingesetzt. Eine abgewandelte Form des Blowfish-Verfahrens bildet außerdem die Grundlage des Passwort-Hashing-Verfahrens bcrypt. Dabei wird die aufwendige Schlüsselinitialisierung gezielt genutzt, um das automatisierte Ausprobieren großer Mengen möglicher Passwörter zu erschweren.

Obwohl für die vollständige Blowfish-Blockchiffre kein allgemein praktikabler Angriff bekannt ist, gilt der Algorithmus heute für neue Anwendungen als nicht mehr empfehlenswert. Der wichtigste Grund ist seine geringe Blockgröße von 64 Bit. Werden unter demselben Schlüssel große Datenmengen verarbeitet, steigt die Wahrscheinlichkeit wiederkehrender Datenblöcke, wodurch bestimmte Angriffe begünstigt werden können. Dieses Problem betrifft auch andere ältere Blockchiffren mit einer Blockgröße von 64 Bit.

Für moderne Verschlüsselungsanwendungen wird deshalb üblicherweise AES (Advanced Encryption Standard) bevorzugt, der mit einer Blockgröße von 128 Bit arbeitet. Blowfish besitzt heute vor allem historische Bedeutung und wird teilweise noch aus Kompatibilitätsgründen unterstützt. Der von Bruce Schneier ebenfalls entwickelte Algorithmus Twofish ist eine eigenständige Weiterentwicklung kryptografischer Konzepte, jedoch kein direkt kompatibler Nachfolger von Blowfish.

Weiterführende Informationen

Twofish, AES, DES, Symmetrische Verschlüsselung, Blockchiffre, Feistel-Netzwerk, bcrypt