**AES (Advanced Encryption Standard)**

Der Advanced Encryption Standard (AES) ist eine Blockchiffre, die als Nachfolger für DES im Oktober 2000 vom National Institute of Standards and Technology (NIST) als Standard bekanntgegeben wurde.

**AES** (Advanced Encryption Standard): Erst kürzlich wurde bei einem Wettbewerb der Algorithmus Rijndael zum neuen Standard erkoren. Schlüssellänge ist 128, 192 oder 256 Bit, die 128 Bit. Bei dem Wettbewerb waren neben der Grundvoraussetzung Sicherheit einige Kriterien: Schnelligkeit, Speicherbedarf, Implementierbarkeit in Chipkarten und in Hardware.

AES schränkt die Blocklänge auf 128 Bit und die Wahl der Schlüssellänge auf 128, 192 oder 256 Bit ein. Die Bezeichnungen der drei AES-Varianten AES-128, AES-192 und AES-256 beziehen sich jeweils auf die gewählte Schlüssellänge. Der Algorithmus ist frei verfügbar und darf ohne Lizenzgebühren eingesetzt sowie in Soft- und Hardware implementiert werden. AES-192 und AES-256 sind in den USA für staatliche Dokumente mit höchstem Geheimhaltungsgrad zugelassen.

im AES ist die Keysize 128 Bit (= 32 Hexziffern)

.

Cipher.getInstance("AES/CBC/PKCS5Padding");

byte[] iv = new byte[16];

.

Key = new SecretKeySpec(b, "AES" );

AES mit MD5-Hash-Key

$ echo hallo | openssl enc -aes-128-cbc -iv 0 -K $(echo passme | openssl md5 -r | cut -c1-32) > secr.txt

openssl enc -d -aes-128-cbc -iv 0 -K $(echo passme | openssl md5 -r | cut -c1-32) < secr.txt

...

**EncFs - Encrypted Filesystem**

Die Dateien und die Dateinamen werden mittels AES verschlüsselt. Die Daten werden durch einen zufälligen AES-Key verschlüsselt. Dieser AES-Key wird verschlüsselt abgespeichert, wobei das Passwort durch vielfaches Hintereinder Ausführen einer Hashfunktion (ca. 100000-mal) ermittelt wird.