Secure hash based encryption

URL

https://www.php-resource.de/script/PHP-Scripte/Sicherheit-mit-PHP/Secure-hash-based-encryption_14015

Produktbild

Image not found or type unknown

Beschreibung

Diese Klasse implementiert eine sicheres Blockverschlüsselungsverfahren, dass im "Output feedback mode" arbeitet **ohne die mcrypt-Bibliothek auskommt**.

Key-Features:
- Benötigt keine mcrypt-Bibliothek.
- Effizientes Verschlüsseln dank Verwendung der sha1() oder md5() Funktionen.
- Die Verschlüsselung ein und des selben Klartexts ergibt immer andere Ausgaben.

Die Sicherheit des Verfahrens beruht auf der nicht Umkehrbarkeit von Hash-Funktionen (sha1 / md5), die als Zufallsgeneratoren verwendet werden. Jeder Block des ursprünglichen Textes wird per binärem XOR mit dem Hash des vorigen Blocks und des letzten verwendeten Schlüssels verknüpft. Als initialier Schlüssel (Initialisierungs Vektor) wird ein per Passwort geschützter Zufallsstring verwendet, der als Präfix der verschlüsselten Nachricht vorangestellt wird. Hier durch kann ein und der selbe Klartext auf verschiedene Weisen verschlüsselt werden.

Details zur Anzeige