Verschlüsselungsstandards

Definitionen und ErklÃ¤rungen Ã¼ber symetrische/asymetrische SchlÃ¼ssel und Hash-Verfahren.

Symetrischer SchlÃ¼ssel

Auf allen Seiten einer Verbindung wird der gleiche SchlÃ¼ssel eingegeben. Dieser eingegebene SchlÃ¼ssel ist die Grundlage zur Erzeugung der verschlÃ¼sselten Verbindung. Diese symetrischenÂ SchlÃ¼ssel haben eine GrÃ¶ÃŸe von 56 - 512Bit.

Symmetrische SchlÃ¼ssel werden wÃ¤hrend einer verschlÃ¼sselten Verbindung verwendet.

Verwendete Algorithmen: DES (56), RC4 (64,128), 3DES (168), AES (128-265)

Asymetrischer SchlÃ¼ssel (Public/Private Key)

Hier gibt es 2 verschiedene SchlÃ¼ssel - den private-key und den public-key. Die Besonderheit dabei beruht in der Tatsache, dass eine mit dem public-key verschlÃ¼sselte Nachricht nur mit dem dazugehÃ¶rigen private-key, und nicht mit dem selben public-key zu entschlÃ¼sseln ist (und umgekehrt). Der public-key wird allgemein ZugÃ¤nglich gemacht und jeder kann ihn benutzen um den Ersteller dieses KeyÃ´s eine verschlÃ¼sselte Nachricht zu senden die nur er (mit seinem private-key) entschlÃ¼sseln kann. Diese SchlÃ¼ssel sind um einiges lÃ¤nger als symetrische, nÃ¤mlich 512 - 4096Bit.

Das ist auch der Grund warum VerschlÃ¼sselungstechnologien das Public-Key-Verfahren fÃ¼r den Verbindungsaufbau benutzenÂ (lÃ¤ngerer Verbindungsaufbau wegen dem lÃ¤ngeren SchlÃ¼ssel) Â und anschlieÃŸend die Verbindung symmetrisch verschlÃ¼sseln. Asymmetrische SchlÃ¼ssel wÃ¤ren fÃ¼r eine permanente Verbindung zu groÃŸ und wÃ¼rden zu viel Bandbreite und Rechenzeit kosten. Zertifikate nutzen ebenfalls das Public-Key-Verfahren.

Verwendete Algorithmen: RSA-Crypto, Diffie-Hellmann, DSA

Hash-SchlÃ¼ssel

Das sind SchlÃ¼ssel mit denen man Daten ver- aber nicht mehr entschlÃ¼sseln kann. Klingt komisch ist aber so!

Die Idee dahinter ist, dass man Daten dadurch signieren kann, d.h. eine VerÃ¤nderung der Daten bewirkt eine Ã„nderung des Hash-Wertes. Da man den Hash-Wert kennt ist so eine Ãœberprüfung der Daten-IntegritÃ¤t (wurden die Daten verÃ¤ndert?) mÃ¶glich.

Hash-Funktionen werden bei der digitalen Signatur (Email), VPN-Verbindungen (IntegritÃ¤t) und bei Passwort-Speicherung (Betriebssystem) verwendet.

Verwendete Algorithmen: MD4, RIPEMD-160, MD5, SHA, SHA1