if(is) internet-sicherheit.

Institut für Internet-Sicherheit - if(is)

Verschlüsselungsverfahren

https://www.internet-sicherheit.de/crypto-poster/

Stand: 26.05.2014
Autor: Dominique Petersen
petersen@internet-sicherheit.de
Grafik: David Bothe
bothe@internet-sicherheit.de

Symmetrisch

Die symmetrische Verschlüsselung verwendet zum Ver- und Entschlüsseln denselben Schlüssel. Da die Schlüssel geheim gehalten oder höchstens zwischen bekannten Kommunikationspartnern ausgetauscht werden, eignen sich die schnellen symmetrischen Verfahren gut für große Datenmengen bei Festplatten- oder Containerverschlüsselung. RC4 kann laut Experten vermutlich live von der NSA gebrochen und entschlüsselt werden. Hier sollten mindestens die Verfahren Camellia oder AES mit jeweils128 Bit verwendet werden.

Extrem unsicher
Unsicher
Mittel
Sicher
Sehr sicher
Maximal sicher

RC4
DES
Triple-DES
Camellia 128
AES 128
Camellia 192
AES 192
Camellia 256
AES 256

Asymmetrisch

Die asymmetrischen Verschlüsselungsverfahren basieren auf je einem öffentlichen (Public Key) und einem geheimen Schlüssel (Private Key), die jeweils dem Ver- und Entschlüsseln dienen. Der Public Key verschlüsselt die Daten, nur mit dem dazugehörigen Private Key lassen sich die Daten korrekt entschlüsseln – umgekehrt auch für die digitale Signatur nutzbar. Verwendung finden diese Verfahren vor allem bei der E-Mail-Verschlüsselung und beim Surfen im Internet (HTTPS, Verifikation von Zertifikaten) sowie bei der Identifikation von Personen (nPA) und Computern. Hierbei sollte mindestens RSA mit 2048 Bit oder ECC mit 192 Bit verwendet werden. Allerdings wurden einige interne ECC-Varianten der NIST von der NSA nachweislich manipuliert, sodass eine Verwendung von ECC allgemein genau geprüft werden sollte.

DSA
(nur signieren)
RSA 1024
RSA 2048
RSA 4096
RSA 8192
ECC 192
(elliptische Kurven NIST)
ECC 224
(elliptische Kurven NIST)
ECC 256
(elliptische Kurven NIST)
ECC 256
(Curve 25519)
ECC 384
(elliptische Kurven NIST)
ECC 521
(elliptische Kurven NIST)

Hash-Funktionen

Hash-Funktionen reduzieren eine beliebige Menge von Daten auf eine Zahl bestimmter Länge (sog. Fingerabdruck, z.B. 160 Bit). Als Einwegfunktionen bieten sie keine praktikable Möglichkeit auf die ursprünglichen Daten zu schließen. Asymmetrische Verfahren sind deutlich langsamer und nicht für größere Datenmengen geeignet, daher sind Hash-Funktionen von zentraler Bedeutung. Beim Verschlüsseln des damit erzeugten Fingerabdrucks mit dem Private Key kann jeder Empfänger mithilfe des Public Keys prüfen, ob die Nachricht tatsächlich vom Absender stammt und nicht durch einen Dritten manipuliert wurde. Werden allerdings gebrochene Verfahren wie MD5 verwendet, können nahezu beliebige manipulierte Nachrichten untergeschoben werden. Daher sollte mindestens ein Verfahren aus der RIPE-MD- und SHA2/3-Familie mit mindestens 256 Bit gewählt werden.

MD5
RIPE-MD 160
SHA1
SHA3 224
SHA2 224
RIPE-MD 256
SHA3 256
SHA2 256
RIPE-MD 320
SHA3 384
SHA2 384
SHA3 512
SHA2 512