DuD
Datenschutz und Datensicherheit

Secure Hash Algorithm (SHA)

Dirk Fox

Secure Hash Standard (SHS)

Am 11.05.2003 veröffentlichte das US-amerikanische National Institute of Standards and Technology (NIST) den weltweit ersten Standard eines kryptographischen Hashverfahrens, den Secure Hash Standard (SHS) [NIST93]. Die Funktionsweise des SHA ist einfach: Ein Datenstrom wird in Abschnitte von 160 bit Länge unterteilt, die nacheinander von einer Kompressionsfunktion verarbeitet werden. Als letzte Ausgabe der Kompressionsfunktion erhält man den gewünschten 160 bit langen Hashwert des Datenstroms.

Das Design der Kompressionsfunktion entscheidet über die kryptographische Stärke, die so genannte Kollisionsresistenz des Hashverfahrens.[1] Als kollisionsresistent gilt eine Hashfunktion dann, wenn es praktisch unmöglich ist, zwei beliebige, nicht notwendigerweise sinnvolle Nachrichten (Bitfolgen) zu finden, die denselben Hashwert besitzen. Wenn diese Bedingung erfüllt ist, dann ist es erst recht unmöglich, zu einem vorliegenden Hashwert eine passende, noch dazu sinnvolle Nachricht zu konstruieren. Gelänge dies, ließen sich digitale Signaturen fälschen: Zu einem vorliegenden, vom „Opfer“ digital signierten Hashwert könnte ein Fälscher eine passende Nachricht mit dem von ihm gewünschten Inhalt erzeugen.

Damgard-Merkle-Prinzip

Bei den meisten der heute verwendeten Hashverfahren, so auch beim SHA, arbeitet der der Kompressionsfunktion zu Grunde liegende Algorithmus nach dem Damgård-Merkle-Prinzip (siehe Abb.) [Damg90]: In 80 „Runden“ je Kompressionsschritt wird ein 512 bit langer Abschnitt M[i] der Nachricht M (für i=1 bis n) über mehrere Bitoperationen mit dem aktuellen Registerinhalt der Kompressionsfunktion verwürfelt – so, dass es keinen effizienten Weg gibt, zwei Datenströme zu finden, die denselben Hashwert ergeben. Gestartet wird die Kompressionsfunktion mit einem Initialisierungsvektor (IV), der im Standard festgelegt wurde; die letzte Ausgabe der Kompressionsfunktion (compress(M[n])) liefert den gewünschten Hashwert der Nachricht (h(M)).

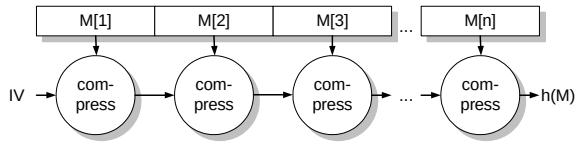

Abb.: Das Damgård-Merkle-Prinzip

Am 17.04.1995 veröffentlichte das NIST auf Grund einer von der National Security Agency (NSA) entdeckten, allerdings unveröffentlichten technischen Schwäche eine korrigierte Version des Algorithmus (SHA-1) [NIST95]. Diese Fassung des SHA ist heute (neben dem inzwischen gebrochenen, aber noch immer gerne verwendeten Hashalgorithmus MD5) das verbreitetste kryptographische Hashverfahren.

SHA-x

Eine Hashfunktion ist nicht nur durch mögliche Schwächen des Algorithmus bedroht. Grundsätzlich kann man zu jeder Hashfunktion Kollisionen finden. Der dafür erforderliche Aufwand lässt sich direkt aus der Länge des Hashwertes ableiten: Ist ein Hashwert 160 bit lang, liegt der Aufwand bei maximal 2^{80} Aufrufen der Hashfunktion. Das ist Resultat des „Geburtstags-Paradoxon“, das ein sehr effizientes Verfahren zur Bestimmung von Kollisionen ermöglicht [DaPr_89].[2]

Am 01.08.2000 publizierte das NIST eine dritte Fassung des Secure Hash Standard als FIPS PUB 180-2. Diese Spezifikation umfasst neben dem SHA-1 drei weitere Algorithmen: SHA-256, SHA-384 und SHA-512, die Hashwerte der Länge 256, 384 und 512 bit erzeugen. Im Rahmen einer „Change Notice“ wurde diese Spezifikation am 25.02.2004 ein weiteres Mal um eine SHA-Variante ergänzt, die 224 bit lange Hashwerte liefert. Diese fünf „SHA-x“-Algorithmen unterscheiden sich nicht nur in der Hashwertlänge, sondern auch in der Größe der verarbeiteten Eingabeblöcke: SHA-1, SHA-224 und SHA-256 verwenden 512 bit lange Blöcke, SHA-384 und SHA-512 verarbeiten 1.024 bit lange Eingaben.

Von der Regulierungsbehörde für Telekommunikation und Post (RegTP) werden die aktuellen Varianten des SHA für qualifizierte Signaturen nach dem deutschen Signaturgesetz empfohlen [RegTP_05].

Quellen

[Damg_90] Damgård, Ivan Bjerre: *A design principle for hash functions*. Proceedings of Crypto ‘89, LNCS 435, Springer, Berlin 1990, S. 416-427.

[DaPr_89] Davies, Donald W.; Price, Wyn L.: *Security for Computer Networks*. 2. Auflage, John Wiley & Sons Ltd., Chichester 1989.

[NIST_93] National Institute of Standards and Technology (NIST): Secure Hash Standard (SHS). Federal Information Processing Standards Publication 180 (FIPS-PUB), 11.05.1993.

[NIST_95] National Institute of Standards and Technology (NIST): *Secure Hash Standard (SHS-1)*. Federal Information Processing Standards Publication 180-1 (FIPS-PUB), 17.04.1995.

[NIST_02] National Institute of Standards and Technology (NIST): *Secure Hash Standard (SHS-2)*. Federal Information Processing Standards Publication 180-2 (FIPS-PUB), 01.08.2002 (Change Notice vom 25.02.2004). http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

[RegTP_05] Regulierungsbehörde für Telekommunikation und Post: *Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen)*, 02.01.2005. http://www.regtp.de/imperia/md/content/tech_reg_t/digisign/198.pdf

[1] Zur Sicherheit von kryptographischen Hashfunktionen siehe Dobbertin, DuD 2/1997, S. 82-87, sowie Weis/Lucks, in diesem Heft.

[2] Zum Geburtstags-Paradoxon siehe Fox, Gateway, DuD 11/2001, S. 684.