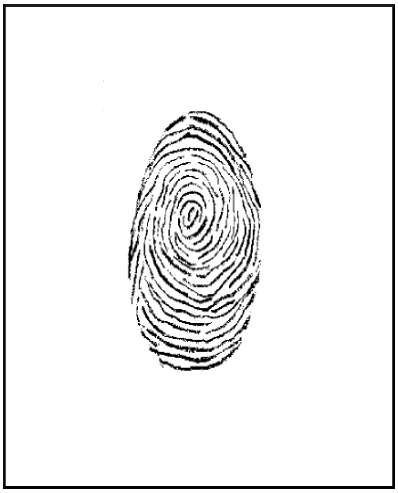
Praktische Anwendung Kryptographischer Prüfsummen



PeterJockisch.de

Peter Jockisch: *Praktische Anwendung kryptographischer Prüfsummen*,
erschienen auf PeterJockisch.de

Stand: 16. März 2014

Peter Jockisch
Habsburgerstraße 11
79104 Freiburg i. Br.
Deutschland

Netzpräsenz: www.peterjockisch.de
E-Post: info@peterjockisch.de

Satz: TEX, LATEX, KOMA-Script
Schrift: Latin Modern

Inhaltsverzeichnis

1 Praktische Anwendung kryptographischer Prüfsummen **2**

1.1 Einleitung . . . 2
1.2 Funktionsweise . . . 3
1.2.1 Elektronische Fingerabdrücke . . . 3
1.2.2 Qualitätskriterien . . . 3
1.2.3 Vorherrschende Standards im Westen und in Rußland . . . 5
1.3 Existieren für die Öffentlichkeit gesperrte Technologien? . . . 5
1.3.1 Veraltete Rechnersysteme . . . 5
1.3.2 Softwareaspekte und Hintertürenproblematik . . . 6
1.4 Anwendungsbeispiele: Geschäftswelt, Internet, Archivierung . . . 6
1.4.1 Wahrung der Dateiintegrität . . . 6
1.4.2 Anhaltspunkt für den Bearbeitungsstand einer Datei . . . 7
1.4.3 Wappnung gegen Wirtschaftskriminalität, Schutz vor Mobbing . . 7
1.4.4 Dateibezugnahme in Verträgen und Eingangsbestätigungen . . . 7
1.4.4.1 Verträge und Empfangsbestätigungen . . . 7
1.4.4.2 Bildlizenzierungen . . . 8
1.4.5 Telefonisch übermittelter Anhaltspunkt für die Echtheit versandter Dokumente . . . 8
1.4.6 Hashwerte-Veröffentlichung als ersatzweiser Echtheitsnachweis . . . 8
1.4.7 Dokumente mit Hashwerten veröffentlichen . . . 9
1.4.8 Archivierung von Dateien . . . 10
1.4.9 Erhöhte Sicherheit bei der Paßwortspeicherung . . . 10
1.4.10 Gesetzlich anerkannte, revisionssichere E-Mail-Archivierung . . . 10
1.4.11 Die qualifizierte elektronische Signatur in der BRD . . . 11
1.4.11.1 Leitfaden Elektronische Signatur . . . 11
1.4.11.2 Signaturgesetzrelevante Begriffsbestimmungen in der BRD 11
1.4.11.3 Offizielle Netzseite der BRD zur Elektronischen Signatur 11
1.4.12 Eine zentrale Netzseite zur angewandten Kryptographie . . . 11
1.4.13 Weitere Anwendungsmöglichkeiten . . . 12
1.4.14 Mißbrauchsmöglichkeiten . . . 12
1.4.14.1 Vollautomatische Identifizierung konsumierter Inhalte . . 12

1.4.15 Softwareaktivierung und Rechneridentifikation über elektronische Fingerabdrücke . . . 13
1.5 Kryptographische Signatur und E-Mail-Zertifikate . . . 13
1.5.1 Kryptographische Signatur und E-Mail-Zertifikate . . . 13
1.5.2 Netzseitenzertifikate-Branche in der Kritik . . . 14
1.6 Signierung und Verschlüsselung von Dateien . . . 14
1.6.1 Realexistierender Schutz mit öffentlich zugelassenen Verschlüsselungsverfahren . . . 14

2 Freie Prüfsummenprogramme 17
2.1 HashCheck . . . 18
2.2 Jacksum . . . 18
2.2.1 Installation von Java und Jacksum . . . 18
2.2.2 Anwendung unter KDE Konqueror und KDE Dolphin . . . 19
2.2.3 GNOME Nautilus . . . 19
2.2.4 Anwendung unter Explorer: MS-Windows 7 . . . 19
2.3 Konsolenbasierte Prüfsummenbildung . . . 20
2.4 RHash . . . 20
2.4.1 Dokumentationsquellen . . . 20
2.5 Bordeigene SHA-Algorithmen unter Unix/BSD- und GNU/Linux-Systemen 20

3 Einführung in die angewandte Kryptographie 23
3.1 Das Prinzip der asymetrischen Verschlüsselung . . . 24
3.2 Mathematische Grundlagen . . . 26

1 Praktische Anwendung kryptographischer Prüfsummen

1.1 Einleitung

Computerdateien können auf viele Weisen unbemerkt manipuliert werden. Kryptographische Prüfsummen, Hashwerte, dienen dem Schutze Ihrer Daten: Durch Bildung eines elektronischen Fingerabdrucks einer Datei wird ein stets gleichbleibender Zahlenwert erstellt. Weicht dieser zu einem späteren Zeitpunkt ab, liegt Beschädigung oder Manipulation vor. Mit einem einzigen Mausklick läßt sich so jederzeit die Unversehrtheit einer Datei prüfen.

Kryptographische Prüfsummen bilden die Grundlage für kryptographische Signierung und Verschlüsselung, für Netzseiten- und E-Mail-Zertifikate, für die qualifizierte elektronische Signatur, sowie für das technische Verständnis der revisionssicheren E-Mail-Archivierung, zu der alle Kaufleute gesetzlich verpflichtet sind.

Diese Einführung stellt drei freie Programme für die Prüfsummenbildung vor: zwei grafisch orientierte, HashCheck und Jacksum, für die Bedienung per Dateimanager sowie das kommandozeilenbasierte[1] RHash. Jacksum und RHash sind betriebssystemplattformübergreifend erhältlich. Eine ausführliche, illustrierte Beschreibung von RHash (Einrichten der Umgebungsvariable, Navigieren in der Verzeichnisstruktur über die Kommandozeile) wird in der nächsten Auflage dieses Artikels erscheinen.

1.2 Funktionsweise

1.2.1 Elektronische Fingerabdrücke

Menschen sind komplexe Lebewesen. Für ihre schnelle und unkomplizierte Identifizierung werden oftmals Fingerabdrücke erstellt. Nach demselben Prinzip können Computerdateien identifiziert werden: durch Erzeugung eines „elektronischen Fingerabdrucks“, der so genannten kryptographischen Prüfsumme, einer stets gleichbleibenden Zahl. Mittels standardisierter Verfahren kann so eine schnelle Integritäts- und Echtheitskontrolle von Dateien jedweder Art vorgenommen werden.

Menschliche Fingerabdrücke werden mit Stempelkissen erstellt, elektronische mit einem Prüfsummenprogramm.

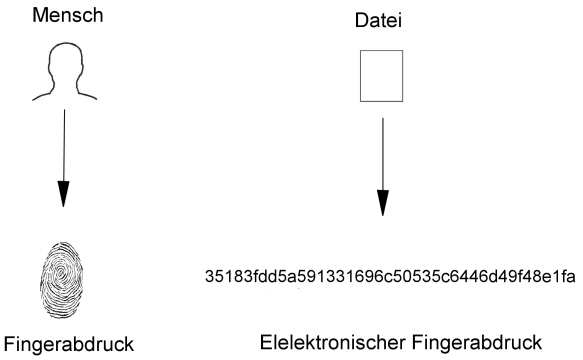


Abb. 1.1: Echtheitsnachweis bei Mensch und Computerdatei

1.2.2 Qualitätskriterien

Wir betrachten *kryptographische* Prüfsummen. Sie basieren auf Streuwert- bzw. Hashfunktionen, die zu einer beliebigen Datei Streu- bzw. Hashwerte als Ergebnis liefern. Dieser Wert wird auch Hashcode bzw. Hash genannt.

Eine Datei, sowie identische Kopien von ihr, weist stets dieselbe Hashwert-Prüfsumme auf. Ändert sich jedoch auch nur ein einziges Bit oder Zeichen durch Beschädigung oder Manipulation, sollte ein gänzlich anderer Hashcode entstehen.

Ein Hashfunktions-Prüfsummenverfahren sollte also zu unterschiedlichen Computerdateien immer unterschiedliche Werte liefern. Die berechnete Prüfsumme ist, abhängig vom verwendeten Verfahren, immer gleichlang. Deshalb kann natürlich nur eine begrenzte Anzahl von Zahlen dargestellt werden: Es gibt praktisch unendlich viele Computer-

dateien, so daß mit einer Zahl fester Länge unmöglich jeder dieser Dateien ein unterschiedlicher Wert zugewiesen werden kann.

Unter Sicherheitsaspekten stellen sich verschiedene Angriffsszenarien dar, unter anderem die Fälschung von Dokumenten. Ein Angreifer möchte von einer gegebenen Originaldatei, beispielsweise einer geschäftlichen Bestellung, eine gefälschte Version mit einer manipulierten, erhöhten Bestellmenge erstellen, welche dieselbe Hashwert-Prüfsumme aufweist. Nachdem er die Änderungen im Dokument vorgenommen hat, versucht er anschließend durch Ausprobieren, vielleicht mittels Einfügung unsichtbarer Steuerzeichen, eine Dateiversion zu erhalten, deren kryptographische Prüfsumme identisch zur derjenigen der Originaldatei ist. Bei solch einem Angriff kommen natürlich unterstützende Computerprogramme zum Einsatz.

Gelingt es nun tatsächlich einem Angreifer, *in zeitlich vertretbarem Aufwand* eine zweite Datei zu erzeugen, die die erwünschten Manipulationen enthält und die dieselbe kryptographische Prüfsumme der Originaldatei aufweist, so ist das betreffende Hashfunktions-Verfahren „gebrochen“. Nach Bekanntwerden solch einer Schwäche sollte es keine Verwendung mehr finden. Durch stetige Forschungsarbeit werden Schwächen schon längere Zeit im voraus erkannt.

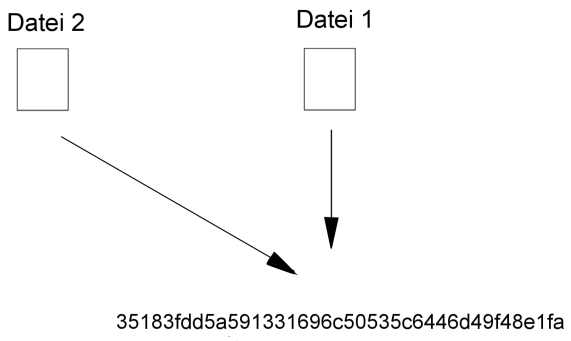


Abb. 1.2: Prüfsummenkollision

Gäbe es einen unendlich berechnungsstarken Computer, so könnte, theoretisch, möglicherweise jedes Verfahren durch schlichtes Ausprobieren sämtlicher Möglichkeiten gebrochen werden (Brute Force Angriff)[2] Für die Praxis wird solch eine Vorgehensweise in der Mehrzahl aller Fälle als nicht praktikabel erachtet, da die erforderlichen Berechnungen fast nie in vertretbarer Zeit durchführbar sind.

Die meisten Hashfunktionen wiesen bisher nur eine begrenzte Lebensdauer auf und wurden irgendwann aus Sicherheitsgründen von Nachfolgeverfahren abgelöst. Berech-

nungsstärkere Computergenerationen tragen zur Verkürzung der Lebensdauer bei. Neben den rechenkraftbasierten Angriffen existieren jedoch auch anders orientierte, und es kann niemals ausgeschlossen werden, daß mithilfe mathematischer Kreativität bereits heute praktikable Angriffe möglich sind.

Im Hintergrund arbeitet und forscht ein riesiges Heer von Mathematikern, insbesondere für Nachrichtendienste. Nicht alle wissenschaftlichen Erkenntnisse werden veröffentlicht.

1.2.3 Vorherrschende Standards im Westen und in Rußland

Die westliche IT-Infrastruktur basiert gegenwärtig noch überwiegend auf dem SHA-1-Algorithmus (Secure Hash Algorithm 1).[3] Dieser ist bereits angebrochen, die erforderliche Rechenzeit, um ihn zu korrumpieren, ist nachweislich gesunken.[4] Der Nachfolgealgorithmus SHA-3 steht bereits seit 2012 offiziell fest.[5]

In Rußland und vielen weiteren GUS-Staaten[6] ist GOST R 34.11-94[7] beziehungsweise GOST 34.311-95[8] der Hash-Standard in Behörden und in der Wirtschaft. „[...] er findet Verwendung beim Einsatz der Digitalen Signatur in Russischen Staatsbanken und Unternehmen. [...]“[9] Wie bereits bei SHA-1 wurden auch beim GOST-Hash strukturelle Schwächen gefunden.[10]

1.3 Existieren für die Öffentlichkeit gesperrte Technologien?

1.3.1 Veraltete Rechnersysteme

Alle berechnungskraftbezogenen Aussagen dieser Einführung beziehen sich auf öffentlich verfügbare bzw. auf für die Allgemeinheit freigegebene Computersysteme und Forschungsarbeiten. Die Nutzung der jeweils aktuellsten, fortgeschrittensten Computertechnologie bleibt gegenwärtig vermutlich noch den Nachrichtendiensten vorbehalten, um diesen stets einen Berechnungskraftvorsprung zu gewährleisten, für eine effektive Aushebelung etablierter Verschlüsselungstechnologie.

Die auf breiter Ebene freigegebenen Verschlüsselungsverfahren mögen für untere Verwaltungsebenen nicht ohne weiteres zu brechen sein. Ganz oben in der Hierarchie, das heißt auf Nachrichtendienstebene, dürfte jedoch ein uneingeschränkter Zugriff auf modernste Computertechnologie vorhanden sein. Zudem werden vermutlich sämtliche über das Weltnetz transferierte Daten archiviert, für eine automatisch erfolgende Auswertung. Unter diesem Aspekt relativiert sich die Widerstandsfähigkeit von über das Internet versandten Dateien, die mit öffentlich standardisierter Technologie verschlüsselt wurden.

1.3.2 Softwareaspekte und Hintertürenproblematik

Schon seit langer Zeit existieren Überlegungen, daß bestimmte zu offiziellen Standards erhobene Kryptographie-Algorithmen inhärente mathematische Schwächen aufweisen könnten, die nur den Experten der Nachrichtendienste bekannt sind. Eine möglicherweise vorhandene Einflußnahme der Geheimdienste auf die Gestaltung von Sicherheitsprodukten (Software- und eventuell Hardware-Hintertürenproblematik, offene Fragen zu Standards usw.) ist Thema zahlreicher Artikel zur Computersicherheit, beispielsweise in „Did NSA Put a Secret Backdoor in New Encryption Standard?“[11] und in „Der Verschlüsselungsstandard AES: Das Danaer-Geschenk der US-Regierung für die Welt?“.[12] Mehrere renommierte Firmen haben bereits direkt oder indirekt bestätigt, bei ihrer Produktentwicklung mit Nachrichtendiensten zusammenzuarbeiten. Offiziell begründet wurde dies unter anderem mit der Absicht, die technische Sicherheit von Firmenprodukten optimieren zu wollen.

Korrumpierte Elektronik, bekannte oder unbekannte „fortschrittliche“ Hardwarearchitekturen mit ab Werk eingebauten „Fernwartungsfunktionen“, möglicherweise sogar mit einem im Prozessor eingebautem Funksystem,[13] stellen, die andere Seite des Problems dar.

1.4 Anwendungsbeispiele: Geschäftswelt, Internet, Archivierung

Auf die umfassenden Voraussetzungen für den *gesetzlich anerkannten* personengebundenen Echtheitsnachweis, der fast immer an die Nutzung von proprietärer[14] Soft- und Hardware gekoppelt ist, wird hier nicht näher eingegangen. Abschnitt 1.4.11 enthält weiterführende Informationsquellen zur so genannten qualifizierten Signatur.

Die Erstellung kryptographischer Prüfsummen gibt nicht nur Anhaltspunkte zur Echtheit und Unversehrtheit von Dateien. Sie ermöglicht auch Empfangsbestätigungen sowie eine schriftliche Bestätigung über den letzten Bearbeitungsstand einer Datei, wie folgende Beispiele demonstrieren

1.4.1 Wahrung der Dateiintegrität

Sie erstellen eine Geschäftsbilanz und gehen anschließend in den Urlaub. Zur Qualitätskontrolle notieren Sie sich vor der Abreise die kryptographische Prüfsumme der fertiggestellten Bilanzdatei. Nach dem Urlaub bilden Sie erneut die Prüfsumme und verifizieren so, ob die Datei unversehrt ist oder ob sie beschädigt oder manipuliert wurde.

Unautorisierte Zugriffe, z. B. auf eine Buchhaltungsdatei, können auf diese Weise entdeckt werden. Benachrichtigen Sie in solchen Fällen die Systemadministratoren und bestehen Sie auf einer Wiederherstellung der ursprünglichen Dateiversion, die natürlich nur dann erfolgreich ist, wenn die Datei wieder die notierte Prüfsumme aufweist.

Die Dateidatumsangabe und Versionsverwaltungssysteme[15] sind kein Ersatz für kryptographische Prüfsummen, da sich beide direkt oder indirekt manipulieren lassen. Spezialisierte Programme, wie beispielsweise die Freeware „Datei-Datums-Änderer“,[16] können sowohl das Erstellungs- als auch das Änderungsdatum von Dateien ändern, sogar verzeichnisweit.

Die Konsistenzprüfung über Prüfsummen funktioniert meist schneller, effektiver und sicherer. Ein separates Prüfsummenprogramm sollte daher immer verfügbar sein.

1.4.2 Anhaltspunkt für den Bearbeitungsstand einer Datei

Beim Verlassen einer Firma möchten Sie sich den letzten Bearbeitungsstand einer Computerdatei schriftlich bestätigen lassen. Hierfür empfehlen sich zwei oder drei verschiedene kryptographische Prüfsummenverfahren. Das ist langfristig möglicherweise sicherer, eines der Verfahren hält vielleicht länger durch in der Zukunft. Auf diese Weise bleibt das Firmengeheimnis gewahrt und Sie können sich trotzdem bis zu einem gewissen Grad absichern. Sollte es jemals Rückfragen geben, haben Sie einen schriftlichen Anhaltspunkt über Ihren letzten Bearbeitungsstand.

1.4.3 Wappnung gegen Wirtschaftskriminalität, Schutz vor Mobbing

Im Rahmen der allgemeinen Qualitätskontrolle und immer dann, wenn Korruption, Lügen, Intrigen, Mobbing, Sabotage und Wirtschaftskriminalität wahrscheinlich werden, empfiehlt sich zum eigenen Schutz der Gebrauch kryptographischer Prüfsummen, auch bei Präsentationen jedweder Art. Signierungssoftware scheidet oftmals aus, da sie naturgemäß mit Verschlüsselungsfunktionen gekoppelt ist und deshalb nicht auf jedem Arbeitsplatzrechner geduldet wird. Firmengeheimnisse könnten verschlüsselt nach außen gelangen bzw. Schadsoftware unentdeckt nach innen. Ein freies[17] Prüfsummenprogramm – nicht zu verwechseln mit Freeware* – kann jedoch verantwortlich auf Firmenrechnern installiert werden.

1.4.4 Dateibezugnahme in Verträgen und Eingangsbestätigungen

1.4.4.1 Verträge und Empfangsbestätigungen

Bei schriftlichen Verträgen und Eingangsbestätigungen erleichtern elektronische Fingerabdrücke die Bezugnahme auf Computerdateien. Dateien jedweder Art können eindeutig über ihren Hashwert identifiziert werden z. B. Textdokumente, Videofilme, *Gesprächsmitschnitte und Interviews* (allgemein Tondateien), Programme, CAD-Dateien. Auch er-

*Der Begriff „Freeware“ ist nicht eindeutig definiert. Er kann sich auf „Freie Software“ (Programmtext/Quellcode[18] ist verfügbar, darf modifiziert und verbreitet werden) beziehen oder auch nicht. Tendentiell vorherrschend bezeichnet er *kostenlos verteilte Software*, deren Programmtext jedoch unveröffentlicht bleibt.

brachte Dienstleistungen, die abschließend in Form eines Datenträgers, z. B. einer abzuliefernden CD-ROM oder DVD vorliegen, lassen sich auf diese Weise schriftlich bestätigen.

Auch von Archivdateien[19] lassen sich elektronische Fingerabdrücke erstellen. Empfangsbestätigungen bilden ein breites Einsatzgebiet.

1.4.4.2 Bildlizenzierungen

In bildgestaltenden Berufsfeldern durchlaufen Fotos bis zur Veröffentlichung viele Nachbearbeitungsphasen, eine Festlegung auf spezifische endgültige Dateien ist im Vorfeld meistens unpraktisch. Referenzdateien können jedoch grundsätzliche künstlerische/bildgestalterische Vorgaben für die Veröffentlichung bzw. langfristige Verwertung verbindlich regeln: Wahl des Bildausschnittes, grundsätzliche Kontrasteigenschaften, implizites Verbot von (weitergehenden) „Schönheitsretuschierungen“ usw. Bildbeschreibungen und Miniaturabbildungen der Originale werden dann samt zugehöriger Dateiprüfsummen im Verwertungsvertrag aufgenommen. Verwenden Sie hierbei möglichst nur solche Dateiformate, die entweder ganz ohne Komprimierung bzw. mit verlustfreier Komprimierung arbeiten, Formate, die auch Farbprofilinformationen speichern können. Bezugnahme auf Referenzfarbräume setzt natürlich ein ordentliches Farbmanagement, eine umfassende Vorbereitung des Geräteparks voraus.

Manchmal sind verbindlich fertiggestaltete Bilddateien möglich. Genügend Auflösungsreserven für die Größenanpassung (Skalierung) vorausgesetzt, können Fotos für eine Internetseite in allen Parametern exakt festgelegt werden. Bei Wahl eines passenden Standards (z. B. TIFF, JPEG, PNG, GIF) ist eine hohe Wahrscheinlichkeit gegeben, daß die Bilder auch noch langfristig von zukünftigen Netzseitenleseprogrammen angezeigt werden können.

1.4.5 Telefonisch übermittelter Anhaltspunkt für die Echtheit versandter Dokumente

Dem Empfänger einer Datei oder eines per Briefpost versandten Datenträgers kann zur Kontrolle telefonisch die Hashfunktions-Prüfsumme mitgeteilt werden. Das Fälschen einer Stimme ist zwar möglich, aber aufwendig. Die personengebundene Signierung wäre jedoch komfortabler und sicherer.

1.4.6 Hashwerte-Veröffentlichung als ersatzweiser Echtheitsnachweis

Manche Staaten erlauben nur eingeschränkt Verschlüsselung und Signierung (personengebundener elektronischer Echtheitsnachweis). Bis zu einem gewissen Grad können kryptographische Prüfsummen als ersatzweiser Notbehelf dienen:

1. Erstellen Sie zunächst *separat* die Nachricht bzw. das Dokument als Computerdatei (Text- oder PDF-Datei, Bild, Video, u. a.). Fügen Sie die Datei einer E-Mail an und versenden Sie die Nachricht.

2. Veröffentlichen Sie auf einer Netzseite tagebuchähnlich die Hashcodes der versandten Dokumente. Mehrere seriöse kostenlose[20] (werbefinanzierte) Webhoster[21] bieten sich dafür an. Auch ohne (X)HTML-Kenntnisse lassen sich Internetseiten erstellen, z. B. mit dem freien grafischen Editor Kompozer.[22]

   Alternativ empfehlen sich kostenlose Blogsysteme, die keine technischen Gestaltungskenntnisse voraussetzen. Ein möglicher kostenloser Dienst ist Blogger.com,[23] ein anderer Wordpress.com.[24] Beide sind einfach und unkompliziert handhabbar und sofort benutzbar, Kommentarfunktionen lassen sich deaktiviert halten. Achten Sie bei Ihrer Auswahl auf eine SSL-/TLS-gesicherte Paßwortübergabe beim Anmeldevorgang, Ihr Benutzerpaßwort sollte immer verschlüsselt über das Internet transportiert werden.

   Ausführliche Grundlageninformationen, auch zu Netztagebüchern (Blogs), finden sich in den Einführungsinformationen für künftige Netzseiteninhaber.[25]

   Erstellen Sie schließlich schematische Einträge, beispielsweise in der Form *Prüfsummenverfahren – Dateiprüfsumme*. Mehr Information bedarf es nicht. Bei umfangreichen täglichen Einträgen könnten Sie optional noch eine Dateinamensabkürzung hinzufügen. Aus dem E-Mailanhang „Anfrage.pdf“ würde dann „A...e.pdf“ oder einfach nur „A...e“ werden.

3. Der Empfänger der Datei kann nun einen Hashwerte-Abgleich vornehmen, indem er Ihre Netzseite bzw. Ihren Blog aufruft und den zugehörigen Hashcode zur symbolisch angedeuteten Nachricht liest.

1.4.7 Dokumente mit Hashwerten veröffentlichen

Für die Veröffentlichung von Dokumenten im Internet oder im Intranet (lokales Firmennetz) empfiehlt sich die Angabe von Hashwerten, eventuell auf einer Unterseite, im so genannten Herunterlade- bzw. „Download“-Bereich. Die Nutzung eines gesetzlich anerkannten SSL-/TLS-Zertifikates[†] zur verschlüsselten Übertragung der Prüfsummen verstärkt die Sicherheit. Durch Abgleichen der Hashwerte können sich Nutzer relativ sicher sein, daß von seriösen Quellen heruntergeladene Dokumente frei von Schadcode (Viren usw.), Manipulationen und Transferschäden sind. Von äußeren Instanzen ausgestellte Zertifikate sind jedoch möglicherweise mit Restrisiken[26] verbunden.

[†] Zertifikate sind Ausweise für das Internet (Netzwerke allgemein), meistens E-Mail- oder Netzseitenzertifikate. Mit ihnen läßt sich die Datenübertragung auch verschlüsseln („https://[...]“), wodurch ein Mitlesen für *unter* dem Gesetz stehende Menschen und Organisationen relativ unmöglich ist (WP-Artikel: „Digitales Zertifikat“).

1.4.8 Archivierung von Dateien

Bei der Datei-Archivierung auf CD-ROMs und DVDs empfiehlt sich die Notierung des Datenträger-Hashcodes. Zur Überprüfung gleichen Sie in regelmäßigen Abständen den Istwert mit dem ursprünglich notierten Hashwert ab. Auf diese Weise können frühzeitige Schäden erkannt werden. Das regelmäßige Umkopieren auf neue archivierungsspezialisierte Datenträger, in relativ kurzen Zeitabständen, ist momentan leider noch unumgänglich.

1.4.9 Erhöhte Sicherheit bei der Paßwortspeicherung

In der Informatik und in der Elektrotechnik existieren zahlreiche weitere Anwendungsmöglichkeiten, beispielsweise eine Variante der sicherheitserhöhten Speicherung von Benutzerkontodaten: Ein Klartextpaßwort läßt sich auch ausschließlich in Form seines zugehörigen Hashwertes speichern. Gibt der Nutzer sein Klartextpaßwort erneut ein, wird der Hashwert erneut gebildet und mit dem gespeicherten abgeglichen. Im Falle eines Dateneinbruchs oder Datendiebstahls gehen so vorerst keine Klartextpaßwörter verloren.

Gute zeitgemäße Streuwertfunktionen wirken wie Einwegfunktionen.[27] Sie weisen einer Datei einen individuellen Hashwert zu. Der umgekehrte Weg, die Berechnung der Originaldatei aus dem Hashwert, ist jedoch nicht in praktikabler Zeit möglich – gemäß gegenwärtigem öffentlich bekanntem Wissensstand.[28]

1.4.10 Gesetzlich anerkannte, revisionssichere E-Mail-Archivierung

In manchen Wirtschaftszweigen werden E-Mails, die zu Geschäftsabschlüssen/-Aufträgen führen, rechtlich als Handelsbriefe[29] betrachtet. Für ihre Archivierung reichen ein einfaches Abspeichern oder Ausdrucken nicht mehr aus, stattdessen muß revisionssicher archiviert werden, auf eine technische Weise, die ein nachträgliches, nicht feststellbares unbemerktes Manipulieren der E-Mail-Daten ausschließt.

Die technische Umsetzung erfolgt vermutlich bei den meisten Programmen mit Hilfe von kryptographischen Prüfsummen. Dabei werden von allen ein- und ausgehenden E-Mails elektronische Fingerabdrücke erstellt und in verschlüsselter Form gespeichert. Möchte z. B. ein Wirtschaftsprüfer Einblick in eine bestimmte E-Mail erhalten, so wird die gespeicherte E-Mail-Datei in das entsprechende E-Mail-Archivierungsprogramm geladen, z. B. von einer CD-ROM. Beim Einlesen wird erneut die kryptographische Prüfsumme der E-Mail-Datei gebildet und mit der ursprünglich archivierten zugehörigen Prüfsumme auf Übereinstimmung verglichen.

Nur ganz bestimmte Software- und/oder Hardwarelösungen von bestimmten Herstellern werden im Rahmen der gesetzlichen Anforderungen rechtlich anerkannt. Im Weltnetz sind zahlreiche hochwertige Einführungsartikel zu diesem Thema erhältlich, verfaßt von spezialisierten Rechtsanwälten und IT-Experten. Eine kleine Auswahl:

- „FAQ der IT-Recht Kanzlei: zu den Themen E-Mail-Archivierung und IT-Richtlinie“[30]
- „Mangelhafte Archivierung elektronischer Post hat Konsequenzen [,] Gesetzliche Vorgaben für die eMail-Archivierung“[31]
- „Rechtssichere E-Mail-Archivierung – Teil 1 Einführung und Rechtsvorschriften“[32]
- WP-Artikel „E-Mail-Archivierung“[33]
- WP-Artikel „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“[34]
- Beispiel für eine kommerzielle softwarebasierte Lösung, mit einem „Leitfaden zur rechtssicheren E-Mail-Archivierung (PDF)“, jeweils für Deutschland, Österreich und die Schweiz erhältlich, „Mailstore Server“: „Vorteile der E-Mail-Archivierung“[35]

1.4.11 Die qualifizierte elektronische Signatur in der BRD

1.4.11.1 Leitfaden Elektronische Signatur

Der „Leitfaden Elektronische Signatur“ von Rolf Schmoldt bietet eine umfassende Einführung in die gesetzlich anerkannte elektronische Signatur in Deutschland.[36]

1.4.11.2 Signaturgesetzrelevante Begriffsbestimmungen in der BRD

Die Netzseite des „Bundesministeriums der Justiz“ zum „Gesetz über Rahmenbedingungen für elektronische Signaturen“ enthält Begriffsbestimmungen.[37]

1.4.11.3 Offizielle Netzseite der BRD zur Elektronischen Signatur

- www.bundesnetzagentur.de → „*Qualifizierte elektronische Signatur*“[38]
- „Gesetze und Bestimmungen“[39]
- „Aktuell tätige Zertifizierungsdiensteanbieter“[40]
- „Häufig gestellte Fragen / FAQ (Frequently Asked Questions)“[41]

1.4.12 Eine zentrale Netzseite zur angewandten Kryptographie

Bert-Jaap Koops' „Cryptography Law Survey“ gibt Auskunft über die grundsätzliche Gesetzeslage zur Kryptographie in den einzelnen Staaten der Welt. Jeder Eintrag ist mit einer umfassenden weiterführenden Quellensammlung versehen: www.cryptolaw.org.

1.4.13 Weitere Anwendungsmöglichkeiten

Prüfsummen werden auch in der Elektrotechnik schon seit vielen Jahrzehnten eingesetzt, unter anderem zur Gewährleistung einer fehlerfreien Datenübertragung.

1.4.14 Mißbrauchsmöglichkeiten

1.4.14.1 Vollautomatische Identifizierung konsumierter Inhalte

Kryptographische Prüfsummen lassen sich auch für fragwürdige Zwecke einsetzen. Der Medienabspieler eines Softwareherstellers soll in der Vergangenheit ungefragt Hashcodes der abgespielten Dateien versandt haben.[42]

Theoretisch ließe sich über einen vollautomatischen Abgleich mit Datenbanktabellen feststellen, ob genutzte Inhalte lizenziert wurden und welche politischen Filme und Tondateien sich ein Nutzer bevorzugt anschaut. Individuelle Rechner könnten durch eine Merkmalkombination identifiziert werden, und Prüfsummen natürlich auch auf Betriebssystemebene versandt werden. Dasselbe wäre auch bei proprietären PDF-Programmen möglich.

Alternativ sind freie PDF-Betrachter[43] und freie Medienabspieler,[44] beispielsweise der sehr empfehlenswerte VLC-Mediaplayer[45] erhältlich. Eine umfassende, größtmögliche Sicherheit setzt jedoch immer auch eine freie Betriebssystembasis[46] voraus.

In der Computerforensik[47] sowie in unzähligen weiteren informationstechnischen Bereichen ist die Bildung bzw. Abfrage kryptographischer Prüfsummen allgegenwärtig. Eine durchaus konstruktive Anwendung, insbesondere auch unter dem Aspekt der Beweissicherung bei Computerdelikten, wie z. B. nach Netzwerkeinbrüchen.

In Diktaturen besteht die Gefahr, daß vor Ort oder aus der Ferne „Festplattendurchsuchungen“ vorgenommen werden. Durch Hintertüren von Software- und Hardwareherstellern können routinemäßig kryptographische Prüfsummen aller vorhandenen Festplattendateien erstellt werden und anschließend vollautomatisch mit den Prüfsummen indizierter[48] und zensierter Inhalte,[49] wie z. B. politischer Aufklärungsfilme, abgeglichen werden. Auf diese Weise kann schnell und effektiv überprüft werden, ob Bürger dazu tendieren, eine eigene Meinung zu pflegen, und ob sie politische Inhalte konsumieren, die im Widerspruch zu offiziell verkündeten Dogmen stehen. Freidenker lassen sich so leicht ausfindig machen.

Bei einem regelmäßigem Versand sämtlicher Prüfsummen neuerstellter sowie geänderter Dateien könnte auch im nachhinein festgestellt werden, in welchem Netzwerk bzw. auf welchem Rechner ein Dokument erstmalig erstellt wurde.

Die Datenmenge ist winzig und, wenn sie zusätzlich verschlüsselt wird, praktisch unentzifferbar. Das Ändern des Dateinamens ändert nicht die Prüfsumme. Auch andere Merkmale, wie z. B. Hardware- und Softwarekonfigurationen (einschließlich nichtlizenzierter Programme), lassen sich analysieren und vollautomatisch „melden“.

Rechtsanwalt Udo Vetter erwähnt in einem Vortrag[50] vom 23.06.2010 eine von der Polizei verwendete Software für die Festplattendurchsuchung, bei der auch schon ein Fehlalarm ausgelöst worden sein soll.‡

1.4.15 Softwareaktivierung und Rechneridentifikation über elektronische Fingerabdrücke

Die Free Software Foundation (FSF)[55] führt in einem Artikel zur Privatsphäre[56] Computermerkmale auf, über die sich ein Rechner eindeutig identifizieren und wiedererkennen läßt. Solche Kenndaten werden in einem Hash zusammengefaßt und in einer Datenbank archiviert. Bei manchen proprietären Produkten ist die Softwareaktivierung (Produktaktivierung)[57] an die ermittelte Hardwarekonfiguration gekoppelt. Der Versuch, die gekaufte Software gleichzeitig auf einem zweiten Rechner zu installieren scheitert dann oftmals.

1.5 Kryptographische Signatur und E-Mail-Zertifikate

1.5.1 Kryptographische Signatur und E-Mail-Zertifikate

In der Vergangenheit versahen Personen bzw. Ämter ihre Dokumente mit einem zusätzlichen Echtheitsnachweis, indem sie mit Siegellack bzw. Sigelwachs und Siegelstempeln[58] komplexe Muster auf die Dokumente auftrugen. Heute übernehmen kryptographische Schlüssel bzw. Zertifikate die Funktion des Siegelstempels: Für ein Dokument, z. B. eine E-Mail-Datei, wird mit Hilfe eines Zertifikates (eines Ausweises) ein begleitender, personengebundener Echtheitsnachweis berechnet, die so genannte kryptographische Signatur. Nach Eingang der Nachricht stellt das E-Mail-Programm des Empfängers (u. a. mit Hilfe dieser Signatur) vollautomatisch fest, ob das Dokument wirklich vom angegebenen Versender (Zertifikatsinhaber/Ausweisinhaber) erstellt wurde.

E-Mail- und Netzseitenzertifikate haben also eine Ausweisfunktion, mit der Korrespondenzpartner und Internetseiten ihre Identität nachweisen können.

Klassische Ausweise werden von staatlichen Behörden ausgestellt. E-Mail- und Netzseitenzertifikate werden von so genannten Zertifizierungsstellen ausgestellt (Certification Authorities, CAs). Und hier liegen die zwei entscheidenden Unterschiede: Klassische Ausweise sind untereinander alle gleichwertig und amtlich anerkannt, es gibt nur einen einzigen Aussteller, der zugleich als Beglaubigungsinstitution fungiert: den Staat.

‡ „Netzwoche Bielefeld – Udo Vetter – Das überwachte Netz“, Einstiegspunkt in der 18. Minute, Direktverweis: http://www.youtube.com/watch?v=2eZrWjhQ06w#t=17m59s. Der gesamte Vortrag ist äußerst aufschlußreich hinsichtlich der „Qualität“ der BRD-„rechtsstaatlichen“ Ermittlungen im Internet- und IT-Bereich. Netzpräsenz von Udo Vetter: www.lawblog.de.[51] Das internationale Menschenrechteportal Wikimannia.org[52] enthält im Personen-Portal[53] einen Kurzportraitartikel[54] zu Udo Vetter, mit Netzverweisen.

E-Mail und Netzseitenzertifikate hingegen existieren in unterschiedlichen Güteklassen, mit unterschiedlicher Aussagekraft. Nur Zertifikate höchster Güteklasse (Class-3-E-Mail-Zertifikate bzw. EV-Netzseitenzertifikate), ausgestellt von staatlich anerkannten Zertifizierungsstellen,[59] werden rechtlich anerkannt.

1.5.2 Netzseitenzertifikate-Branche in der Kritik

Die internationale Netzseiten-Zertifikateaussteller-Branche in ihrer Gesamtheit sieht sich mittlerweile schwerer Kritik ausgesetzt. Zum einen, weil es immer wieder vorkommt, daß einzelne CAs an Unberechtigte Zertifikate vergeben, aufgrund mangelhafter Überprüfungsverfahren bei der Antragsstellung. Zum anderen aufgrund von erfolgten Hackereinbrüchen durch die es Dritten zeitweise unbemerkt gelang, sich formal anerkannte Zertifikate auszustellen, für verschiedene populäre Internetseiten. Die Kritik läßt sich dahingehend zusammenfassen, daß die gegenwärtige technische Grundlage des Zertifikatesystems zu verletzlich ist für solche Fehler und Angriffe, und daß mir ihr nicht effektiv und schnell genug Gegenmaßnahmen ergriffen werden können. Suchbegriffe wie SSL-GAU, SSL-Desaster, oder englisch SSL debacle führen auf Diskussionsbeiträge und auf weiterführende Artikel im Weltnetz. Umfangreiche Informationsquellen: CA/Browser Forum: www.cabforum.org; „The EFF SSL Observatory“: www.eff.org/observatory.

1.6 Signierung und Verschlüsselung von Dateien

1.6.1 Realexistierender Schutz mit öffentlich zugelassenen Verschlüsselungsverfahren

Es kann nicht ausgeschlossen werden, daß offiziell empfohlene, zu Standards erhobene Kryptographie-Algorithmen inhärente mathematische Schwächen aufweisen, um Nachrichtendiensten die Entschlüsselung zu erleichtern. Vermutlich wird wirklich fortgeschrittene Computertechnologie der Öffentlichkeit vorenthalten bzw. allgemein gesperrt gehalten, um Geheimdiensten einen Berechnungskraftvorsprung zu garantieren. Unter diesem Aspekt und angesichts der höchstwahrscheinlich vorhandenen Einflußnahme auf die Firmenproduktgestaltung (Software- und Hardware-Hintertürenproblematik) ist die Effektivität der realexistierenden Verschlüsselungspraxis fragwürdig; auch dann, wenn durchgängig offene, freie IT-Infrastruktur zum Einsatz kommt.

Konsequent angewandte Signierung und Verschlüsselung wehren jedoch zumindest einen Teil des infragekommenden Personenkreises möglicher Geschäftsangreifer ab und verhindern einen direkten Datenzugriff bei Diebstahl und Verlust von Datenträgern.

Endnoten

1. WP-Artikel „Kommandozeile“: http://de.wikipedia.org/wiki/Kommandozeile.
2. „Brute-Force-Methode“: http://de.wikipedia.org/wiki/Brute-Force-Methode.
3. Spezifikation zu SHA-1: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf und http://tools.ietf.org/html/rfc3174.
4. „Hash mich – Konsequenzen der erfolgreichen Angriffe auf SHA-1“, Reinhard Wobst, Jürgen Schmidt, Heise Security, Stand: 18.02.2005: www.heise.de/security/artikel/Konsequenzen-der-erfolgreichen-Angriffe-auf-SHA-1-270648.html. „Attacken auf SHA-1 weiter vereinfacht“, 11.06.2009, http://www.heise.de/security/meldung/Attacken-auf-SHA-1-weiter-vereinfacht-180587.html. Technology Review, „Algorithmus ohne Geheimnisse“, Erica Naone, 25.11.2008: http://www.heise.de/tr/artikel/Algorithmus-ohne-Geheimnisse-275852.html.
5. Heise.de, 03.10.2012, „Sieger im Kryptographie-Wettbewerb steht fest“: http://www.heise.de/newsticker/meldung/Sieger-im-Kryptographie-Wettbewerb-steht-fest-1722483.html. golem.de, 03.10.2012: „Hash-Algorithmus für SHA-3 festgelegt“, www.golem.de/news/keccak-hash-algorithmus-fuer-sha-3-festgelegt-1210-94887.html.
6. GUS-Staaten: http://www.cis.minsk.by.
7. Spezifikation GOST R 34.11-94: http://tools.ietf.org/html/draft-dolmatov-cryptocom-gost341194-07.
8. GOST-Standards: http://www.gost.ru/wps/portal/pages.en.Main.
9. 02. Februar 2014, http://rhash.anz.ru/hashes.php: „GOST is a hash function defined in Russian national standard GOST R 34.11-94. It has two widely used versions with testparameters and CryptoPro ones. It’s relatively slow, but it is used for digital signature in Russian State banks and enterprises. Hash is a hexadecimal string of length 64.“
10. Heise-Verlag News-Meldung vom 20. August 2008: www.heise.de/security/meldung/oesterreichische-Kryptologen-attackieren-Hasvh-Funktionen-197880.html.
11. „Did NSA Put a Secret Backdoor in New Encryption Standard?“, Bruce Schneier, 15. November 2007 auf Wired.com: www.wired.com/politics/security/commentary/securitymatters/2007/11/securitymatters_1115.
12. „Der Verschlüsselungsstandard AES: Das Danaer-Geschenk der US-Regierung für die Welt?“, recentr.com, 06. Januar 2013: http://recentr.com/2013/01/der-verschlusselungsstandard-aes-das-danaer-geschenk-der-us-regierung-fur-die-welt.
13. Kopp-Online 28.09.2013: „»Geheimer« 3G-Chip von Intel ermöglicht Schnüfflern Zugriff auf Computer“.
14. „proprietär“: http://de.wikipedia.org/wiki/Propriet%C3%A4r.
15. „Versionsverwaltung“: http://de.wikipedia.org/wiki/Versionsverwaltung.
16. Programm „Datei-Datums-Änderer“: http://www.chip.de/downloads/Datei-Datums-aenderer_44961498.html.
17. „Freie Software“: http://de.wikipedia.org/wiki/Freie_Software.
18. „Quelltext“: http://de.wikipedia.org/wiki/Quelltext.
19. „Packprogramme“ dienen der Erstellung von Archivdateien bzw. Dateiarchiven, kurz „Archiv“ genannt. Sie bieten insbesondere die Möglichkeit, mehrere Einzeldateien sowie verschachtelte (das heißt Unterordner enthaltende) Dateiordner zu einer einzigen Datei zusammenzufassen. Dadurch können beispielsweise ganze Weltnetzseiten und umfangreiche persönliche Zusammenstellungen von Dokumenten komfortabel als einzelne Datei einem E-Brief beigefügt werden, oder auf einen Datenträger gebrannt werden.
„Packprogramm“: http://de.wikipedia.org/wiki/Packprogramm,
Packprogrammempfehlung 7zip: http://de.wikipedia.org/wiki/7zip,
Freie Datenkompressionsprogramme: Kategorie:Freie Datenkompressionssoftware.
20. „Comparison of free web hosting services“: http://en.wikipedia.org/wiki/Comparison_of_free_web_hosting_services.
21. „Webhosting“: http://de.wikipedia.org/wiki/Webhosting.
22. Netzseiteneditor Kompozer: http://www.kompozer-web.de.
23. WP-Artikel „Blogger.com“: http://de.wikipedia.org/wiki/Blogger.com.
24. Kostenlose Weltnetztagebücher bei Wordpress.com: http://de.wordpress.com/features.
25. „Einführungsinformationen für künftige Netzseiteninhaber“: http://peterjockisch.de/Empfehlungen-zu-Freier-Software/Empfehlungen-zu-Freier-Software.html#Informationen-fuer-kuenftige-Netzseiteninhaber.
26. Heise Security News-Meldung vom 25.03.2010: „EFF zweifelt an Abhörsicherheit von SSL“, www.heise.de/security/meldung/EFF-zweifelt-an-Abhoersicherheit-von-SSL-963857.html.
27. „Einwegfunktion“: http://de.wikipedia.org/wiki/Einwegfunktion.
28. Ein Grundlagenartikel zu Paßwörtern: Daniel Bachfeld, „Cracker Bremse [...]“, 03.06.2011, http://www.heise.de/security/artikel/Passwoerter-unknackbar-speichern-1253931.html?view=print.
29. „Handelsbrief“: http://de.wikipedia.org/wiki/Handelsbrief.

30. „FAQ der IT-Recht Kanzlei: zu den Themen E-Mail-Archivierung und IT-Richtlinie“: http://www.it-recht-kanzlei.de/faq-email-archivierung.html.
31. „Mangelhafte Archivierung elektronischer Post hat Konsequenzen [,] Gesetzliche Vorgaben für die eMail-Archivierung“: http://www.it-business.de/index.cfm?pid=2454pk=151661p=1.
32. „Rechtssichere E-Mail-Archivierung – Teil 1 Einführung und Rechtsvorschriften“: http://www.perspektive-mittelstand.de/Rechtssichere_E_Mail_Archivierung____Teil_1_Einf_hrung_und_Rechts/management-wissen/1279.html.
33. „E-Mail-Archivierung“: http://de.wikipedia.org/wiki/E-Mail-Archivierung.
34. „Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen“: http://de.wikipedia.org/wiki/GDPdU.
35. „Vorteile der E-Mail-Archivierung“: http://www.mailstore.com/de/mailstore-server-vorteile.aspx.
36. „Leitfaden Elektronische Signatur“: http://www.signature-perfect.de/docs/Leitfaden_Elektronische_Signatur.pdf.
37. „Gesetz über Rahmenbedingungen für elektronische Signaturen“: http://www.gesetze-im-internet.de/sigg_2001/index.htmlBJNR087610001BJNE000201308.
38. Bundesnetzagentur, „Qualifizierte elektronische Signatur“: http://www.bundesnetzagentur.de/cln_1931/DE/Service-Funktionen/QualifizierteelektronischeSignatur/qualifizierteelektronischesignatur-node.html.
39. Bundesnetzagentur, „Gesetze und Bestimmungen“: http://www.bundesnetzagentur.de/cln_1911/DE/Service-Funktionen/QualifizierteelektronischeSignatur/GesetzlicheGrundlagen/Rechtsgrundlagen_node.html.
40. Bundesnetzagentur: „Aktuell tätige Zertifizierungsdiensteanbieter“: http://www.bundesnetzagentur.de/cln_1931/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/AufsichtundAkkreditierungvonAnbietern/01_Auflistung_aktuelle_ZDA.html.
41. Bundesnetzagentur, „Häufig gestellte Fragen / FAQ (Frequently Asked Questions)“: http://www.bundesnetzagentur.de/cln_1931/DE/Service-Funktionen/QualifizierteelektronischeSignatur/FAQ/faq-node.html.
42. Heise.de-Nachricht, 21. Februar 2002, „Windows Media Player: Ich weiß, was du letzten Sommer geschaut hast“: http://www.heise.de/newsticker/meldung/Windows-Media-Player-Ich-weiss-was-du-letzten-Sommer-geschaut-hast-56439.html,
Richard M. Smith, 20.02.2002, „Serious privacy problems in Windows Media Player for Windows XP“: http://www.computerbytesman.com/privacy/wmp8dvd.htm,
Businessweek.com, 14. Februar 2000, NEWS: ANALYSIS COMMENTARY, „The Privacy War of Richard Smith“: http://www.businessweek.com/2000/00_07/b3668067.htm.
43. Zwei umfassende Übersichten zu freien PDF-Betrachtern: „Entscheiden Sie sich für einen Freien PDF-Betrachter!“: http://www.pdfreaders.org,
WP-Artikel „Category:Free PDF readers“: http://en.wikipedia.org/wiki/Category:Free_PDF_readers.
44. „Kategorie:Freier Medienspieler“: http://de.wikipedia.org/wiki/Kategorie:Freier_Medienspieler.
45. „VLC media player“: http://de.wikipedia.org/wiki/VLC_media_player.
46. „Category:Free software operating systems“: http://en.wikipedia.org/wiki/Category:Free_software_operating_systems.
47. „IT-Forensik“: http://de.wikipedia.org/wiki/Computerforensik.
48. „Bundesprüfstelle für jugendgefährdende Medien“: http://de.wikipedia.org/wiki/Bundespr%C3%BCfstelle_f%C3%BCr_jugendgef%C3%A4hrdende_Medien.
49. „Zensur im Internet“: http://de.wikipedia.org/wiki/Zensur_im_Internet.
50. „Netzwoche Bielefeld – Udo Vetter – Das überwachte Netz“, Einstiegspunkt in der 18. Minute: http://www.youtube.com/watch?v=2eZrWjhQ06w.
51. „law blog“: http://www.lawblog.de.
52. „Wikimannia.org“: http://de.wikimannia.org/Hauptseite.
53. „Personen-Portal“: http://de.wikimannia.org/Portal:Personen.
54. „Udo Vetter“: http://de.wikimannia.org/Udo_Vetter.
55. Free Software Foundation: www.fsf.org.
56. „Privatsphäre und Microsoft“: http://de.windows7sins.org/privacy.
57. „Produktaktivierung“: http://de.wikipedia.org/wiki/Produktaktivierung.
58. „Siegel“: http://de.wikipedia.org/wiki/Siegel.
59. Bundesnetzagentur: „Aktuell tätige Zertifizierungsdiensteanbieter“: http://www.bundesnetzagentur.de/cln_1931/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/AufsichtundAkkreditierungvonAnbietern/01_Auflistung_aktuelle_ZDA.html.

2 Freie Prüfsummenprogramme

Aus der großen Menge freier grafischer Prüfsummenprogramme heben sich Jacksum[1] und HashCheck[2] hervor. Jacksum, veröffentlicht unter einer OSI-zertifizierten[3] Freie-Software-Lizenz, der GPL, gelistet im FSF-Verzeichnis[4] und basierend auf Java,[5] läuft auf vielen Betriebssystemplattformen. Es eignet sich damit auch für heterogene IT-Infrastrukturen[6] von Firmennetzwerken. Zahlreiche international gängige Prüfsummenverfahren werden berücksichtigt, die Dateimanagerintegration gewährleistet eine komfortable Bedienung.

Jacksum-Dateimanagerversionen sind erhältlich für GNOME, KDE, ROX und Thunar (Unix/BSD, GNU/Linux) sowie für den Explorer von MS-Windows [7] und den Finder von Apple Macintosh. Vom Programmautor, Johann Löfflmann, wird eine Netzseite[8] mit ausführlichen Informationen zu Jacksum gepflegt. Vorschläge zur Programmerweiterung („feature request“) können eingereicht werden, der Austausch unter den Nutzern wird ebenfalls gefördert.[9]

HashCheck, eine Erweiterung für den MS-Windows Dateimanager „Explorer“, bietet nur einen Bruchteil der Algorithmen, unterstützt jedoch ebenfalls den SHA1-Algorithmus und funktioniert auch ohne Java.

Unter den plattformübergreifenden Textmodus-Programmen für GNU/Linux und MS-Windows zeichnet sich RHash[10] aus, das wie Jacksum die Bildung des im osteuropäischen Raum weitverbreiteten GOST-Hashes unterstützt.

Eine vergleichende Übersicht zu zahlreichen freien und proprietären Prüfsummenprogrammen findet man im WP-Artikel „Comparison of file verification software“.[11] Grundlegende Begriffe und zentrale Verweise zu freier Software werden im Artikel „Einführung in Freie Software und Betriebssysteme“[12] aufgeführt.

2.1 HashCheck

HashCheck ist eine freie Dateimanagererweiterung[13] für den MS-Windows-Explorer. Laden Sie sich HashCheck entweder über die offizielle Projektseite[14] herunter, oder über ein renommiertes Programmeverzeichnis, z. B. beim „Heise Software Verzeichnis“.[15]

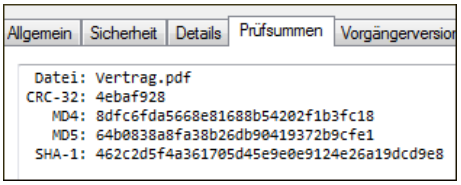


Abb. 2.1: Datei und Prüfsummen

Nach der Installation bilden Sie die Prüfsumme(n) zu einer Datei wie folgt: Fahren Sie mit dem Mauszeiger auf die von Ihnen gewünschte Datei. Drücken Sie die rechte Maustaste und wählen Sie „Eigenschaften“, wodurch sich ein Fenster öffnet. Klicken Sie dann auf die Reiterkarte[16] „Prüfsummen“, woraufhin der SHA1-Prüfsummenwert der Datei angezeigt wird.

Weitere Funktionen werden auf der Projektseite beschrieben. Die Benutzerschnittstelle von HashTab unterstützt insgesamt 20 Sprachen, laut der offiziellen Netzpräsenz. Weitere Informationen: FAQ,[17] Bildschirmfotos.[18]

2.2 Jacksum

Jacksum kann über den Dateimanager oder als Kommandozeilenprogramm aufgerufen werden. Die Dateimanagerversion setzt keine installierte Kommandozeilenversion voraus, sie arbeitet unabhängig.

Im folgenden wird die Anwendung unter GNOME,[19] KDE[20] und MS-Windows Explorer[21] beschrieben. Auf die Benutzung unter ROX,[22] Thunar[23] und Finder[24] wird im offiziellen Fragen- und Antworten-Bereich der Jacksum-Netzpräsenz eingegangen.[25]

2.2.1 Installation von Java und Jacksum

In Unix- und unixartigen Betriebssystem-Distributionen ist Java[26] meistens schon enthalten, in der freien[27] Variante OpenJDK.[28] Als MS-Windows-Benutzer rufen Sie eine Suchmaschinenseite auf, zum Beispiel Google, und tippen „Java“ oder „JRE“ ein, das ist die Kurzbezeichnung für „Java Runtime Environment“ (Java-Laufzeitumgebung).[29] Dieser Schritt entfällt, wenn bereits eine Java-Laufzeitumgebung vorhanden ist.

Installation und Anwendung von Jacksum werden ausführlich im Herunterladebereich[30] der offiziellen Programmseite beschrieben sowie in den dem Jacksum-Download beigefügten readme.txt-Dateien. Das jeweilige Dateimanagermenü kann variieren, je nach ausgewählten Installationsoptionen. Debian- bzw. Ubuntu-Nutzer können die Kommandozeilenversion über die Paketverwaltung herunterladen (versionsabhängig, z. B.: *System* → *Systemverwaltung* → *Synaptic-Paketverwaltung*).[31]

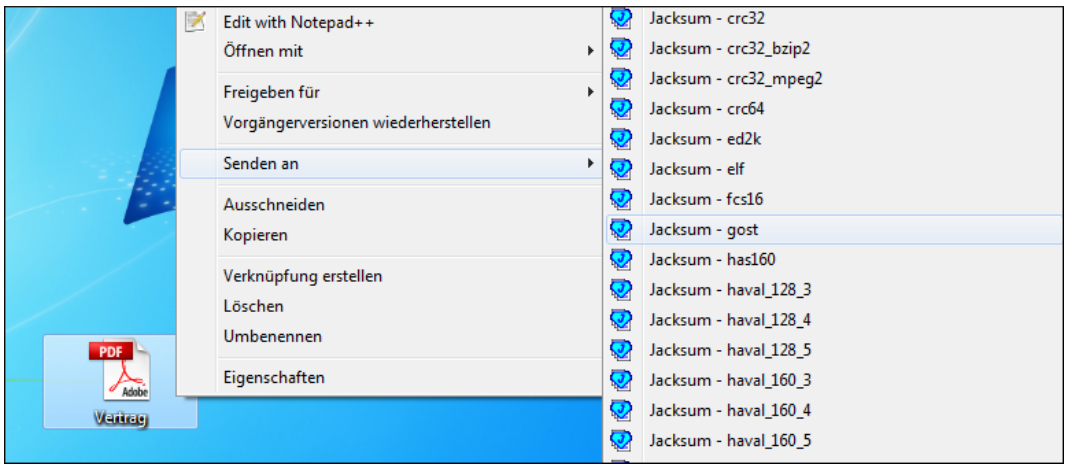


Abb. 2.2: Jacksum unter MS-Windows 7

2.2.2 Anwendung unter KDE Konqueror und KDE Dolphin

Öffnen Sie den Dateimanager. Klicken Sie zum Wählen der Datei auf die *rechte Maustaste* → *„Aktion“* → *„Jacksum“* → [gewünschte Funktion wählen].

2.2.3 GNOME Nautilus

Öffnen Sie den Dateimanager. Klicken Sie zum Wählen der Datei auf die *rechte Maustaste* → *„Skripte“* → *„Jacksum“* → [gewünschte Funktion wählen].

2.2.4 Anwendung unter Explorer: MS-Windows 7

Besorgen Sie sich Jacksum auf jonelo.de.[32] Im Download-Bereich laden Sie die Windows-Explorer-Integration herunter (bei Bedarf zusätzlich die Kommandozeilenversion). Entpacken und installieren Sie das Programm.

Der zugehörige Hashwert einer Datei wird unter MS-Windows 7 gebildet, indem man mit der rechten Maustaste auf die ausgewählte Datei klickt, „Senden an“ wählt, dann auf „Jacksum“ geht und zum Schluß den gewünschten Prüfsummenalgorithmus auswählt. Prüfsumme sowie Dateiname samt Verzeichnispfad erscheinen in einem separaten Fenster und können kopiert werden. Mit „--3) Alle Algorithmen“ werden die Werte aller Verfahren auf einmal angezeigt.

Die Anwendungsmöglichkeiten von Jacksum sind zahlreich. Über die Kommandozeilenversion entfaltet sich das ganze Potential dieser vorzüglichen Software, einschließlich der Interaktion mit anderen Programmen. Die Bereitstellung einer offenen Programmschnittstelle (API)[33] fördert die breite Akzeptanz.

2.3 Konsolenbasierte Prüfsummenbildung

Die Nutzung der Befehlszeilenumgebung[34] ermöglicht ein hocheffektives Arbeiten am Computer. Manche Anwendungen werden ausschließlich für den heutzutage meist emulierten Textmodus[35] geschrieben, andere bieten zusätzlich zur grafischen auch eine textbasierte Programmschnittstelle.[36]

Seit der Einführung von Microsoft's Windows PowerShell[37] können MS-Windows-Nutzer neben den klassischen MS-DOS-Befehlen[38] (erweitert in cmd.exe)[39] standardmäßig auch grundlegende Dateioperationsbefehle der BSD/Unix-Welt[40] nutzen (Gegenüberstellung).[41]

2.4 RHash

RHash[42] ist ein leistungsfähiges, plattformübergreifend[43] erhältliches Kommandozeilenprogramm, das viele Prüfsummenverfahren[44] unterstützt, darunter auch den SHA1- sowie den GOST-Hash. Durch seine Plattformunabhängigkeit (BSD/Unix, GNU/Linux, MS-Windows) eignet es sich hervorragend für die Nutzung innerhalb von heterogenen IT-Firmennetzwerken.

2.4.1 Dokumentationsquellen

Offizielle Seite,[45] Manual,[46] Dokumentationswiki,[47] Hashfunktionen,[48] Lizenz.[49]

2.5 Bordeigene SHA-Algorithmen unter Unix/BSD- und GNU/Linux-Systemen

SHA-Algorithmen sind standardmäßig auf Unix- und unixartigen Systemen vorinstalliert. Öffnen Sie eine Befehlszeilenumgebung (Shell), schreiben Sie „sha“ und drücken Sie dann die Tabulatortaste für die Autovervollständigung, um sich alle vorhandenen SHA-Verfahren anzeigen zu lassen:

```
> sha
> sha1sum  sha224sum  sha256sum  sha384sum  sha512sum  shasum
> sha
```

Gehen Sie in das entsprechende Verzeichnis, wählen Sie ein Verfahren, fügen Sie den Namen der gewünschten Datei an und drücken Sie die Eingabetaste. Im folgenden Beispiel wird die SHA1-Prüfsumme der Datei test.html gebildet:

```
> sha1sum test.html
4a204c74e481facb40fe674c4e23917d6dedf064  test.html
>
```

Der SHA1-Prüfsummenwert und der Name der zugehörigen Datei werden angezeigt. Implementierung und Befehlsbezeichnungen können variieren. Praktisch alle Unix- bzw. unixartigen Systeme und Distributionen verfügen über entsprechende Vorinstallationen. Es gibt dutzendfach freie Programme zur Bildung kryptographischer Prüfsummen, sowohl grafische wie auch textbasierte, u. a. bei www.sourceforge.net. Das freie, konsolenbasierte und plattformübergreifend erhältliche Programm ReHash[50] kann ebenfalls den GOST-Hash bilden, neben zahlreichen weiteren[51] Prüfsummenalgorithmen. Textbasierte Programme ermöglichen die effektivste Nutzung von Computern. Einen hervorragenden Überblick bietet Andreas Poisel's www.automatisch.cc.

Endnoten

1. Offizielle Netzseite zu Jacksum: http://www.jonelo.de/java/jacksum/index_de.html.
2. HashCheck-Projektseite: http://code.kliu.org/hashcheck.
3. Open Source Initiative, „Licenses by Name“: www.opensource.org/licenses/alphabetical.
4. Free Software Directory, Jacksum: http://directory.fsf.org/project/jacksum.
5. Wikipedia-Artikel „Java (Programmiersprache)“: http://de.wikipedia.org/wiki/Java_(Programmiersprache), http://de.wikipedia.org/wiki/OpenJDK.
6. „Heterogenität (Informationstechnik)“: http://de.wikipedia.org/wiki/Heterogenit%C3%A4t_%28Informationstechnik%29.
7. „[...] funktioniert mit dem Explorer unter Windows NT/2000/2003/XP/2008/Vista/7 [...]“, Quelle (Stand: 17. Januar 2014): www.jonelo.de/java/jacksum/index_de.html#Download.
8. Jacksum-Netzpräsenz: http://www.jonelo.de/java/jacksum/index_de.html.
9. Englischsprachige Seitenversion zu Jacksum: www.jonelo.de/java/jacksum/index.html.
10. Offizielle Seite zu RHash: http://rhash.anz.ru.
11. „Comparison of file verification software“: http://en.wikipedia.org/wiki/Comparison_of_file_verification_software
12. „Einführung in freie Software und Betriebssysteme“: http://www.peterjockisch.de/texte/computerartikel/Einfuehrung-in-Freie-Software-und-Betriebssysteme/Einfuehrung-in-Freie-Software-und-Betriebssysteme.html.
13. „Dateimanager“: http://de.wikipedia.org/wiki/Dateimanager.
14. Offizielle Hashcheck-Netzpräsenz: http://code.kliu.org/hashcheck.
15. HashCheck im Heise Software Verzeichnis: http://www.heise.de/download/hashcheck-1169338.html.
16. „Registerkarte“: http://de.wikipedia.org/wiki/Registerkarte.
17. „HashCheck Shell Extension - FAQ“: http://code.kliu.org/hashcheck/faq.html.

18. „Bildschirmfotos zu HashCheck“: http://code.kliu.org/hashcheck/screenshots.
19. „Gnome“: http://de.wikipedia.org/wiki/GNOME.
20. „KDE“: http://de.wikipedia.org/wiki/KDE.
21. „Windows-Explorer“: http://de.wikipedia.org/wiki/Windows-Explorer.
22. „ROX-Desktop“: http://de.wikipedia.org/wiki/ROX_Desktop.
23. „Thunar“: http://de.wikipedia.org/wiki/Thunar.
24. „Finder (Mac)“: http://de.wikipedia.org/wiki/Finder_%28Mac%29.
25. Fragen- und Antworten-Bereich der Jacksum-Netzpräsenz: http://www.jonelo.de/java/jacksum/index_de.html#FAQ.
26. „Java-Technologie“: http://de.wikipedia.org/wiki/Java-Technologie.
27. „Freie Software“: http://de.wikipedia.org/wiki/Freie_Software.
28. WP-Artikel „OpenJDK“: http://de.wikipedia.org/wiki/OpenJDK.
29. „Java-Laufzeitumgebung“: http://de.wikipedia.org/wiki/Java-Laufzeitumgebung.
30. Herunterladebereich der Jacksum-Netzpräsenz: http://www.jonelo.de/java/jacksum/index_de.html#Download.
31. Ubuntu Packages, Paket: jacksum (1.7.0-2) [universe]: http://packages.ubuntu.com/de/lucid/jacksum.
32. Jacksum-Netzseite: http://www.jonelo.de/java/jacksum/index_de.html.
33. Programmschnittstelle bzw. „Programmierschnittstelle“: http://de.wikipedia.org/wiki/Programmierschnittstelle.
34. WP-Artikel „Kommandozeile“: http://de.wikipedia.org/wiki/Kommandozeile.
35. „Textmodus“: http://de.wikipedia.org/wiki/Textmodus.
36. Programmschnittstelle bzw. „Programmierschnittstelle“: http://de.wikipedia.org/wiki/Programmierschnittstelle.
37. „Windows PowerShell“: http://de.wikipedia.org/wiki/Windows_Powershell.
38. „MS-DOS“: http://de.wikipedia.org/wiki/MS-DOS.
39. „cmd.exe“: http://de.wikipedia.org/wiki/Cmd.exe.
40. „Unix-Kommando“: http://de.wikipedia.org/wiki/Unix-Kommandos.
41. „Windows PowerShell [...] Cmdlets“: http://de.wikipedia.org/wiki/Windows_PowerShell#Cmdlets.
42. RHash-Netzpräsenz: http://rhash.anz.ru.
43. „Plattformunabhängigkeit“: http://de.wikipedia.org/wiki/Plattformunabh%C3%A4ngigkeit.
44. Rhash – Unterstützte Hashfunktionen: http://sourceforge.net/apps/mediawiki/rhash/index.php?title=Hash_functions.
45. Offizielle HashCheck-Netzseite: http://rhash.anz.ru.
46. HashCheck-Manual: http://rhash.anz.ru/manpage.php.
47. HashCheck-Dokumentationswiki: http://sourceforge.net/apps/mediawiki/rhash/index.php?title=Main_Page.
48. Von HashCheck unterstützte Hashfunktionen: http://rhash.anz.ru/hashes.php.
49. HashCheck-Lizenz: http://rhash.anz.ru/license.php.
50. Offizielle ReHash-Seite: http://rehash.sourceforge.net.
51. ReHash Hilfe: http://rehash.sourceforge.net/rehash.html.

3

Einführung in die angewandte Kryptographie

In der Vergangenheit versah man Dokumente mit aufwendig gestalteten Siegeln, um ihre Echtheit zu bestätigen. Heute werden kryptographische Signaturen als begleitender Echtheitsnachweis zu Computerdateien berechnet. Kryptographische Signaturen sind also personengebundene Echtheitsnachweise die bestätigen sollen, daß ein versandtes Dokument auch wirklich vom Ersteller bzw. vom Absender stammt.

Verschlüsselung ermöglicht es, gespeicherte bzw. zu versendende Computerdateien unleserlich zu machen, damit Dritte keinen Zugriff auf die Inhalte bekommen.

Gegenwärtig ist der effektive Schutz, der mit öffentlich verfügbarer Kryptographietechnologie erlangt werden kann, äußerst fragwürdig. Fortschrittliche Computertechnologie wird höchstwahrscheinlich für die Öffentlichkeit gesperrt gehalten, um den Nachrichtendiensten der Herrschenden stets einen Berechnungskraftvorsprung zu gewährleisten. Zudem existieren vermutlich Software- und Hardware-Hintertüren. Offiziell empfohlene standardisierte Verschlüsselungsverfahren weisen möglicherweise inhärente mathematische Schwächen auf: Wieso sollten die Nachrichtendienste der westlichen und östlichen Hemisphäre selbstentwickelte sichere Algorithmen empfehlen und verschenken, deren Gebrauch ihre zentrale Arbeit, das Abhören und die Wirtschaftsspionage, verunmöglichen würde?

Die *höherrangigen* Organisationen derjenigen Familien, die über dem Gesetz stehen, verfügen höchstwahrscheinlich über eine unvergleichbar starke Berechnungskraft, der Normalanwender nur wenig entgegenzusetzen haben. Ein Teil derjenigen möglichen Angreifer, die unter dem Gesetz stehen, kann jedoch abgewehrt werden. Die Kommunika-