fhwedel
UNIVERSITY OF APPLIED SCIENCES

Technisches Seminar SS2018

Thema: Grundkonzepte der asymmetrischen Kryptographie

Eingereicht von: Mardjan Awis (Winf100909)

****

****

E- Mail: winf100909@stud.fh-wedel.de

Abgegeben am: 05.07.2018

Betreuer: Prof. Dr. Michael Anders

Fachhochschule Wedel

Feldstraße 143

22880 Wedel

Tel.: +49 4103 8048 48

E- Mail: an@fh-wedel.de

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abb.	Abbildung
bzw.	beziehungsweise
i.d.R	in der Regel
sog.	so genannt
z.B.	zum Beispiel
bspw.	beispielsweise

Abbildungsverzeichnis

1. Einleitung

Das Wort Kryptographie entstammt aus dem Altgriechischen und setzt sich aus den Worten *kryptós*, „verborgen“, und *gráphein*, „schreiben“ zusammen. Dies lässt auch auf den ursprünglichen Sinn, der Verschlüsselung von Informationen („Geheimschriften“) schließen. Mit Beginn des digitalen Zeitalters wurde das Feld der Kryptographie erweitert, unter anderem mit den Bereichen Authentizität und Datenintegrität. Heutzutage beschäftigt sich die Kryptographie nun fast ausschließlich mit dem Schutz von Daten durch deren Transformation, in der Regel unter Einbeziehung von geheimen Schlüsseln. Bis heute ist es jedoch so, dass die fähigsten Menschen, die sich mit Kryptografie und Kryptoanalyse auskennen den Geheimdiensten angehören. Besonders heikel ist, dass Geheimdienste die Ausarbeitung von Verschlüsselungstechniken unterwandert und Fehler einbauen, die sich wie Hintertüren auswirken und für die Überwachung genutzt werden.

Kryptographie verfolgt diverse Schutzziele wie Vertraulichkeit, Integrität, Nachrichtenauthentizität, Teilnehmerauthentizität und Verbindlichkeit. Die kryptographischen Methoden, mit welchen man diese Ziele sicherstellen kann, werden in zwei Kategorien eingeteilt: in symmetrische und asymmetrische Verfahren. Bei dem symmetrischen Ansatz besitzen beide Parteien A und B denselben geheimen Schlüssel k, welcher vorab über einen vertraulichen und authentischen Kanal ausgetauscht werden muss. Bei dem asymmetrischen Ansatz hingegen besitzt jeder Teilnehmer A und B ein eigenes Schlüsselpaar (e, d), bestehend aus einem öffentlichen Schlüssel e und einem dazugehörigen privaten Schlüssel d. Der öffentliche Schlüssel eines Teilnehmers wird vor dem eigentlichen Nachrichtenaustausch über einen authentischen Kommunikationskanal an den entsprechenden Kommunikationsteilnehmer übermittelt. Im Gegensatz zum symmetrischen Ansatz muss die Übertragung des öffentlichen Schlüssels nicht geheim sein. Aufgrund dieser Eigenschaft werden asymmetrische Verfahren auch als Public-Key-Verfahren bezeichnet.

Bei digital elektronischem Datenaustausch spricht man oft von der digitalen Unterschrift (digitale Signatur), welche ein Mittel gegen Verfälschungen ist. Digitale Signaturen basieren in der Regel auf asymmetrischen Verfahren, wo mit dem privaten Schlüssel unterschrieben wird und mit einem öffentlichen Schlüssel die Signatur auf die Authentizität überprüft wird. Im Folgenden wird es, neben den asymmetrischen Kryptographieverfahren, auch um digitale Signaturen gehen.

2. Geschichtlicher Hintergrund

Im Vergleich zu symmetrischen Verschlüsselungsverfahren, sind asymmetrische Verfahren relativ jung. Existierten schon zur Zeit des großen Cäsars entsprechender symmetrische Verfahren, kamen erst in den 1970er Jahren erste asymmetrische Kryptosysteme auf den Markt.
Den ersten Schritt zur Entwicklung asymmetrischer Verfahren machte Ralph Merkle 1974 mit dem nach ihm benannten Merkles Puzzle, das aber erst 1978 veröffentlicht wurde. Das erste Public-Key-Verschlüsselungsverfahren war das von Ralph Merkle und Martin Hellman entwickelte Merkle-Hellman-Kryptosystem. Das MH-Verfahren wurde 1983 von Adi Shamir gebrochen. Im Sommer 1975 veröffentlichten Whitfield Diffie und Martin Hellman eine Idee zur asymmetrischen Verschlüsselung, ohne jedoch ein genaues Verfahren zu kennen. Unter dem Einfluss dieser Arbeit entwickelten Diffie und Hellman im Jahr 1976 den Diffie-Hellman-Schlüsselaustausch.
Das erste asymmetrische Verschlüsselungsverfahren wurde 1977 von Ronald L. Rivest, Adi Shamir und Leonard M. Adleman am MIT entwickelt und nach ihnen RSA-Verfahren genannt. Nach heutiger Terminologie ist dieses Verfahren eine Falltürpermutation, die sowohl zur Konstruktion von Verschlüsselungsverfahren als auch von Signaturverfahren eingesetzt werden kann.

3. Asymmetrische Kryptographieverfahren

3.1 Notwendigkeit

Die große Schwachstelle bei symmetrischen Verschlüsselungsverfahren/Secret-Key-Verfahren ist der Schlüsselaustausch. Denn nicht nur der Geheimtext, sondern auch der Schlüssel muss zum Empfänger gelangen. Der nötige Transport ist unsicher und angreifbar. Davon abgesehen müssen beide Personen den Schlüssel geheim halten; sie werden beide potenzielle Opfer von Angriffen. Weiterhin benötigt jedes Sender-Empfänger-Paar einen eigenen geheimen Schlüssel, wenn man optimale Sicherheit gewährleisten will.
Bei 12 Teilnehmern wären das zwar noch 66 benötigte Schlüssel. Bei 1 000 jedoch schon 499 500 Schlüssel und bei 1 000 000 Teilnehmer praxisferne 49 999 950 000

nötige Keys. Die Schlüsselanzahl wächst folglich quadratisch mit der Teilnehmerzahl. Um eine solche hohe Schlüsselzahl zu verhindern, könnte man z. B. 100 Teilnehmern den gleichen Schlüssel nutzen lassen. Der Nachteil dabei liegt aber auf der Hand: Höhere Unsicherheit. 2 Teilnehmer können ein Geheimnis/den Key besser bewahren als 100; von dem Transport ganz abgesehen.

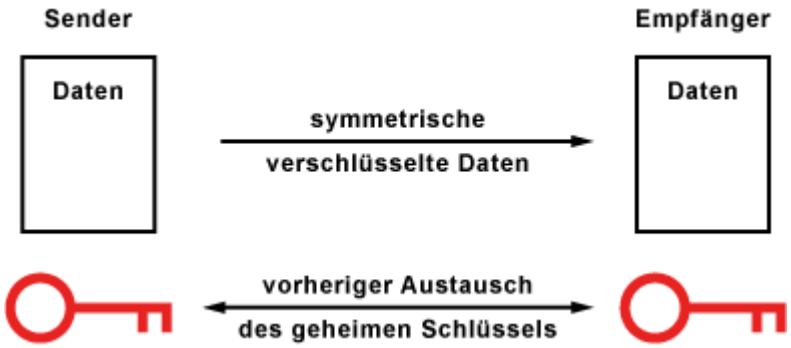

Abbildung 1: Symmetrische Verschlüsselung

3.2 Prinzip

Asymmetrische Verschlüsselungsverfahren arbeiten mit Schlüsselpaaren. Ein Schlüssel ist der öffentliche Schlüssel (Public Key), der andere ist der private Schlüssel (Private Key). Dieses Schlüsselpaar hängt über einen mathematischen Algorithmus eng zusammen. Daten, die mit dem öffentlichen Schlüssel verschlüsselt werden, können nur mit dem privaten Schlüssel entschlüsselt werden.

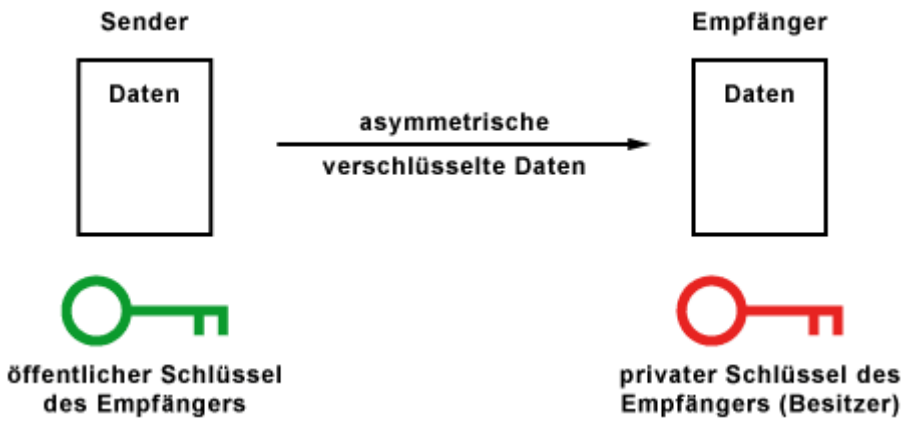

Abbildung 2: Asymmetrische Verschlüsselung

Deshalb muss der private Schlüssel vom Besitzer des Schlüsselpaares geheim gehalten werden. Der konkrete Anwendungsfall sieht so aus: Will der Sender Daten

verschlüsselt an den Empfänger senden, benötigt er den öffentlichen Schlüssel des Empfängers. Mit dem öffentlichen Schlüssel können die Daten verschlüsselt, aber nicht mehr entschlüsselt werden (Einwegfunktion). Nur noch der Besitzer des privaten Schlüssels, also der richtige Empfänger kann die Daten entschlüsseln. Wichtig bei diesem Verfahren ist, dass der private Schlüssel vom Schlüsselbesitzer absolut geheim gehalten wird. Kommt eine fremde Person an den privaten Schlüssel muss sich der Schlüsselbesitzer ein neues Schlüsselpaar besorgen.
So beginnt das Ganze eigentlich mit der Veröffentlichung des, wie der Name es schon sagt, öffentlichen Schlüssels. Die Veröffentlichung kann z.B. über einen Server erfolgen, oder aber auch per Mail. Man muss ihn nicht auf einen sicheren Weg übertragen, jeder darf in den Besitz des öffentlichen Schlüssels gelangen. Oft ist es sogar wünschenswert, dass sich der öffentliche Schlüssel global verteilt, um so sicherzustellen, dass kein anderer öffentlicher Schlüssel unter falschen Namen Verbreitung findet

3.2.1 Einwegfunktion und Falltürfunktion

Bei der asymmetrischen Verschlüsselung geht es darum, eine Funktion zu wählen, die sehr einfach zu rechnen ist, aber deren Umkehrung dagegen sehr aufwendig. Realisiert wird das mit Modulo-Rechenarten. Einige davon sind tatsächlich sehr einfach zu rechnen, während die Umkehrung sehr aufwendig ist. Sie entsprechen also einer Einwegfunktion.
Es gibt allerdings auch Funktionen, bei denen sich mit einer zusätzlichen Information die Umkehrung abkürzen lässt. In so einem Fall spricht man von einer Falltürfunktion. Der diskrete Logarithmus fällt hier als Einwegfunktion besonders auf, weil man diesen sehr leicht berechnen kann. Umgekehrt ist es schlichtweg nicht möglich eine große Zahl in praktikabler Zeit zurückzurechnen. Man bezeichnet das als Diskreter-Logarithmus-Problem. Viele asymmetrische Verfahren basieren darauf. Allerdings bedeutet das nicht, dass nicht doch irgendwann ein Weg gefunden wird, den diskreten Logarithmus zu lösen.
Eine weitere Einwegfunktion ist das Multiplizieren von Primzahlen. Während die Multiplikation für einen Computer kein Problem darstellt, ist der umgekehrte Weg, beim dem das Primzahlprodukt in seine Faktoren zerlegt werden soll, nicht in akzeptabler Zeit machbar. Man spricht von Faktorisierung und in dem

Zusammenhang vom Faktorisierungsproblem. Ein Beispiel: Wenn man 17 x 19 berechnet (beides Primzahlen), dann kommt 323 heraus. Und jetzt soll man die beiden unbekannten Faktoren (17 und 19) daraus zurückberechnen. Es gibt im Prinzip nur einen Weg. Man muss alle Möglichkeiten durchprobieren. Bei hinreichend großen Primzahlen dauert das ewig. Damit ist das Faktorisierungsproblem gemeint.
Alle gängigen asymmetrische Verfahren basieren auf komplexen mathematischen Berechnungen, die gemeinsam haben, dass es für sie noch keine Vereinfachung gibt. Schlüssel, Klartext und Geheimtext stellen große Zahlen bzw. Zahlenpaare dar. Die Verfahren sind aber nur so lange sicher sind, bis jemand eine Vereinfachung gefunden hat. Weil es nur begrenzt geeignete mathematische Berechnungen mit Einwegfunktion gibt, lassen sich nicht beliebig viele asymmetrische Verfahren entwickeln.

3.2.2 Mögliche Angriffe

Angriffe sind unerlaubte und nichtautorisierte Aktivitäten zum Schaden von Ressourcen, Dateien und Programmen oder zum Abfangen und Manipulieren von Informationen und Schlüsseln. Ein möglicher Angriff wäre der Chosen-Cipertext-Angriff. Bei diesem Angriff schickt der Angreifer einen beliebigen Geheimtext an sein Ziel, um diesen entschlüsseln zu lassen. Auch ein Public-Key-Only-Angriff ist denkbar. Mit Wissen des öffentlichen Schlüssels kann der Angreifer beliebigen Klartext verschlüsseln und beispielsweise mit bereits verschlüsselten Klartext vergleichen.
Der vermutlich bekannteste Angriff ist jedoch der Man-In-The-Middle-Angriff. Der Angreifer, versucht dabei den Kommunikationskanal unter seine vollständige Kontrolle zu bringen, und zwar in der Art und Weise, dass die Kommunikationspartner nicht feststellen können ob sie miteinander oder mit dem Angreifer kommunizieren. Der Angreifer hat die Kontrolle über den Datenverkehr, kann die ausgetauschten Informationen einsehen und diese manipulieren.

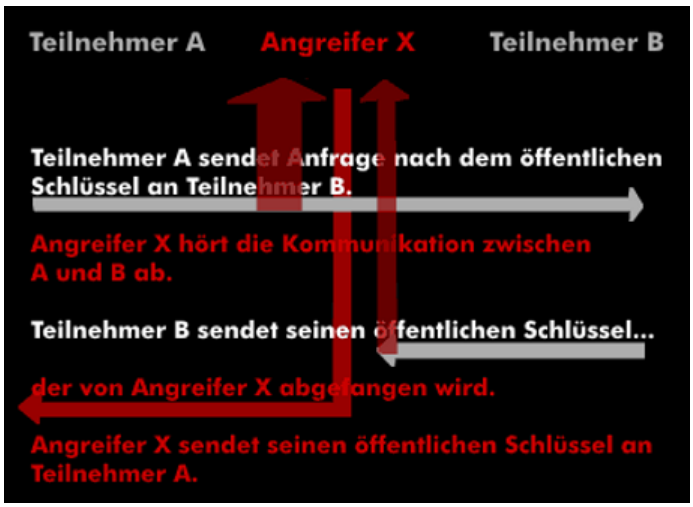

Abbildung 3: Schlüsselmissbrauch (Man-In-The-Middle)

3.3 Anwendung

Anwendung finden asymmetrische Verfahren bei Verschlüsselungen, Authentifizierungen und der Sicherung der Integrität. Bekannte Beispiele, die auf asymmetrische Verfahren aufbauen, sind OpenPGP oder auch S/MIME. Aber auch kryptografische Protokolle wie SSH, SSL/TLS oder auch https bauen auf asymmetrische Kryptosysteme. Eine weitere wichtige Anwendung findet bei digitalen Signaturen statt, worauf im Folgenden noch weiter eingegangen wird.

3.4 Vor- und Nachteile

Ein großer Vorteil von Public-Key-Verfahren ist die hohe Sicherheit. Der Private Key zum Entschlüsseln verbleibt beim Empfänger. Dadurch trägt nur eine Person das Geheimnis und ist angreifbar. Weiterhin ist die Schlüsselverteilung problemlos. Zum einen ist keine Übertragung des Private Keys durch unsichere Kanäle nötig. Zum anderen ist es ebenso nicht notwendig, den Public Key gegen Abhören abzuhärten, da er Angreifern wenig nützt. Das Brechen der Verschlüsselung, also das Entschlüsseln ohne den Private Key, kann Monate bis Jahre dauern. Bis dahin kann die Nachricht schon lange ihre Aktualität verloren haben. Obwohl der Algorithmus bekannt ist, ist der Rechen- und Zeitaufwand zu hoch, um das Verfahren zu brechen. Die heutzutage üblichen 300-stellige Schlüssel wurden faktisch noch nicht geknackt. "Lediglich" 193-stellige konnte man nach einem Jahr Arbeit brechen. Auch ie

Möglichkeit zur Authentifikation durch digitale Signierungen ist von erheblicher Bedeutung. Ein letzter Vorteil ist die Tatsache, dass die Schlüsselzahl nur linear zur Teilnehmerzahl wächst. Ergo werden viel weniger Schlüssel benötigt als bei der symmetrischen Verschlüsselung.

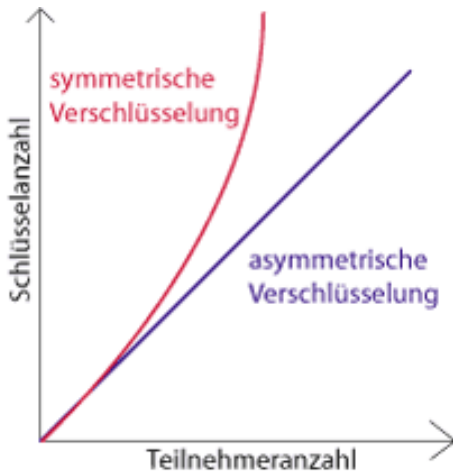

Abbildung 4: Verhalten von Schlüsseln zu Teilnehmern bei verschiedenen Verfahren

Aber auch asymmetrische Verfahren haben ihre Nachteile, wie bspw. eine hohe Rechenzeit. So sind asymmetrische Verschlüsselungen ca. 1000 Mal langsamer als symmetrische. Außerdem liegt ein erhöhter Aufwand bei mehreren Empfängern vor. Da die Verschlüsselung mit dem individuellen Public Key eines jeden Empfängers erfolgt, muss die Nachricht für jeden Empfänger einzeln verschlüsselt werden.

Des Weiteren beruht die Sicherheit von Public-Key-Verfahren auf unbewiesenen Annahmen. Es wäre durchaus möglich, dass man eines Tages einen Algorithmus entdeckt, mit dem man schnell und in kurzer Zeit Zahlen faktorisieren kann. Man vermutet weiterhin, dass man alle Einwegfunktionen mit ausreichend Rechen- und Zeitaufwand umkehren kann - auch 300-stellige Schlüssel. Gelungen ist es bis dato aber noch nicht. RSA ist also nur so lange sicher, wie die (momentane) Unfähigkeit große Zahlen in vernünftiger Zeit zu faktorisieren.

Das Problem mit dem Mittelsmann-Angriff/Man-In-The-Middle ist ebenfalls von Nachteil. Um dies zu verhindern, muss gewährleistet sein, dass der erhaltene Public Key auch wirklich authentisch, also dem gewünschten Empfänger zugehörig, ist. Dazu dienen Zertifikationsstellen, an denen die Public Keys hinterlegt werden und über die man deren Authentizität prüfen kann.

4. Hybride Verfahren

Die hybriden Verschlüsselungsverfahren sollen den Verschlüsselungsaufwand und die langsame De- und Entchiffrierung der asymmetrischen Verschlüsselung kompensieren. Sie kombinieren die Vorteile der symmetrischen Verschlüsselung, nämlich die höhere Bearbeitungsgeschwindigkeit durch schnellere Algorithmen, mit denen der asymmetrischen Verschlüsselung, mit dem öffentlichen Schlüsselaustausch. Deshalb wird für den Nachrichtenaustausch die symmetrische Verschlüsselung benutzt, für den Schlüsselaustausch asymmetrische Verfahren.
Bei der Hybrid-Verschlüsselung wird zunächst ein Sitzungsschlüssel für eine symmetrische Verschlüsselung erzeugt. Dieser Session Key wird für gewöhnlich nur für eine Sitzung generiert. Er wird mit dem öffentlichen Schlüssel verschlüsselt und dem Empfänger übermittelt. Die Nachrichten werden mit dem Sitzungsschlüssel chiffriert und an den Empfänger übertragen. Dieser dechiffriert mit seinem privaten Schlüssel aus dem übermittelten Sitzungsschlüssel einen Schlüssel zur Dechiffrierung der verschlüsselten Nachrichten.
Verschlüsselungsverfahren, die mit dieser Technik arbeiten sind u.a. Pretty Good Privacy (PGP) und S/MIME.

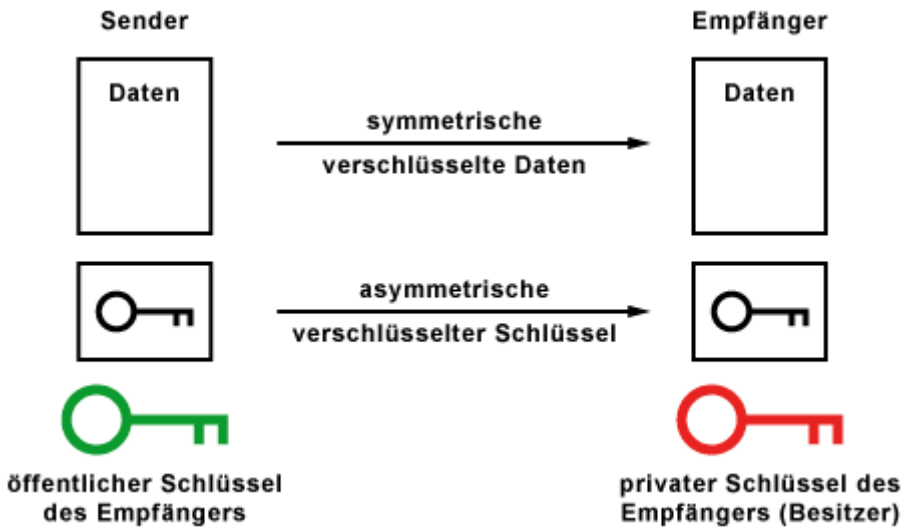

Abbildung 5: Hybride Verschlüsselung

5. Digitale Signatur

5.1 Allgemeines zu digitalen Signaturen

Die digitale bzw. elektronische Signatur ist eine schlüsselabhängige Prüfsumme, die von einer Nachricht oder einem Dokument in Kombination mit einem Schlüssel erzeugt wird. Wird die Signatur an eine Nachricht oder ein Dokument angehängt, dann gilt das als unterschrieben. Im Signaturgesetz (SigG) ist die digitale Signatur wie folgt definiert:

„Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde versehen ist und den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt.“

Für digitale Nachrichten und Dokumente werden solche Signaturen verwendet, um ihre Echtheit glaubhaft und prüfbar zu machen. Die Echtheit der Signatur kann elektronisch geprüft werden. Digitale Signaturen sind in der Datenübertragung deshalb notwendig, weil sich der Absender von Nachrichten und Dokumenten fälschen lässt. Beispielsweise ist es ganz einfach den Absender einer E-Mail zu fälschen. Das heißt, es ist möglich, dass sich jemand als eine andere Person ausgibt. Auch im wirklichen Leben kann man eine beliebige Absender-Adresse auf einen Brief schreiben. Um die Glaubwürdigkeit des Briefs zu unterstreichen setzen wir an das Briefende unsere Unterschrift. Genauso wird es mit der digitalen Signatur gemacht.

5.2 Anforderungen

Damit die elektronische Signatur einer handschriftlichen Unterschrift gleichgesetzt werden kann, muss sie dieselben Eigenschaften wie diese haben. Unterschriften dienen der Identifikation des Unterzeichners, der Echtheit eines Dokuments, dem Abschluss eines Dokuments und der Warnung an den Unterzeichner. Um diese Eigenschaften zu erfüllen, müssen folgende Anforderungen an die elektronische Signatur gestellt werden:

- **Überprüfbar**: Der Empfänger kann einfach überprüfen, dass die Nachricht von dem Unterzeichner unterschrieben wurde.
- **Nicht fälschbar**: Nur der Unterzeichner kann die Signatur an das Dokument anhängen.
- **Nicht wiederverwendbar**: Man kann nicht einfach eine Unterschrift von einem Dokument entfernen und an ein anderes anhängen.
- **Unveränderbar**: Nach der Unterzeichnung ist das Dokument nicht mehr veränderbar (Datenintegrität)
- **Nicht zurücknehmbar**: Die Unterschrift kann nicht zurückgenommen werden. (Verbindlichkeit).

5.3 Verfahren

Vom Verfahren her wird für das Dokument der Hashwert ermittelt und mit dem geheimen Schlüssel des Benutzers verschlüsselt. Dieses neu verschlüsselte Dokument wird mit dem Originaldokument übertragen. Der Empfänger berechnet ebenfalls den Hashwert aus dem Originaldokument, entschlüsselt mit dem öffentlichen Schlüssel das verschlüsselte Dokument und vergleicht beide.

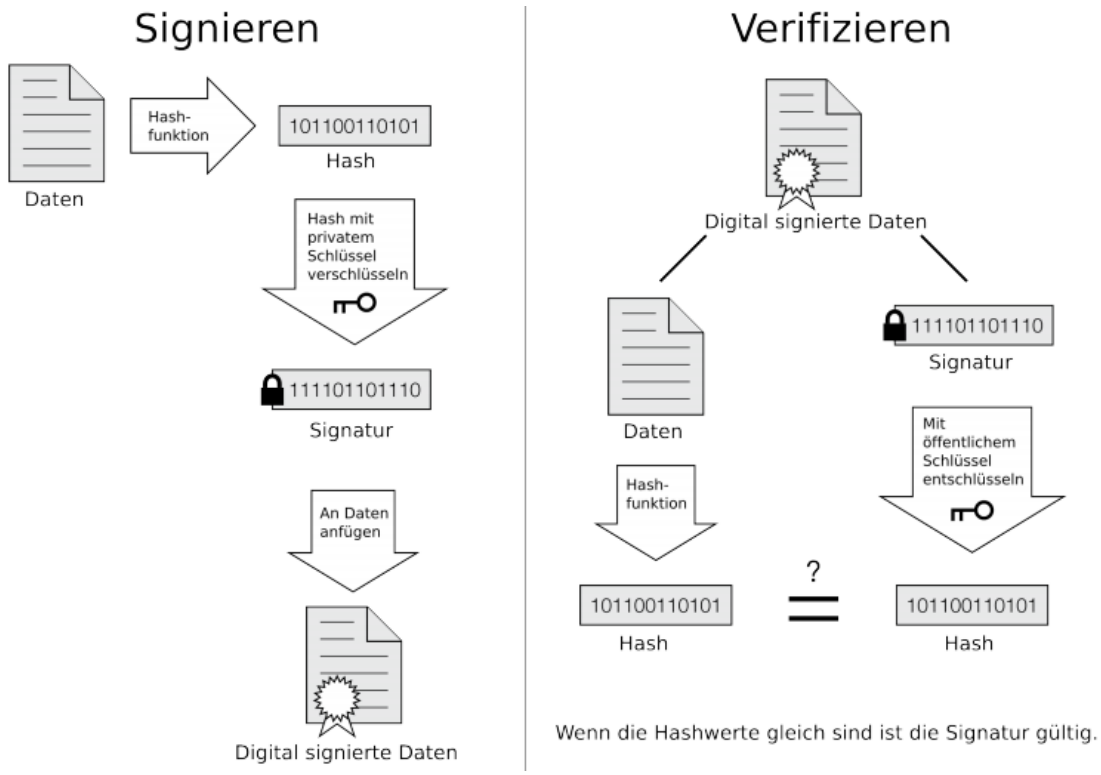

Abbildung 6: Verfahren einer digitalen Signierung

5.4 Der DSA-Algorithmus

Digital Signature Algorithm (DSA) ist eine asymmetrische Verschlüsselung zur Erzeugung und Authentifizierung von digitalen Signaturen. Er wurde 1991 von der National Security Agency (NSA) zusammen mit dem National Institute of Standards and Technology (NIST) entwickelt und 1993 als US-Patent angemeldet. 1994 wurde er schließlich standardiesiert. Die RSA-Verschlüsselung verwendet als Hashfunktion den Secure Hash Algorithm (SHA). Beim DSA-Algorithmus handelt es sich um eine Weiterentwicklung des ElGamal-Algorithmus und OpenSSL. Basis für die Berechnung der diskreten Logarithmen ist dabei eine mathematische Modulo-Operation mit einer großen Primzahl. Da die Rechenleistung zur Entschlüsselung des Algorithmus extrem hoch ist, geht man davon aus, dass der DSA-Algorithmus sicher ist. Zumindest solange bis das Gegenteil bewiesen ist.

5.5 Public Key Infrastructure

Unter einer Sicherheitsinfrastruktur, einer Public Key Infrastructure (PKI), versteht man eine Umgebung in der Services zur Verschlüsselung und zur digitalen Signatur auf Basis von Public-Key-Verfahren bereitgestellt werden. Bei dieser Sicherheitsstruktur wird der öffentliche Schlüssel eines Zertifikatnehmers (ZN) mit

den entsprechenden Identifikationsmerkmalen durch eine digitale Signatur von einer Zertifizierungsinstanz (CA) autorisiert. Die Instanzen der Sicherheitsinfrastruktur sind für das gesamte Schlüssel-Management zuständig. Der Einsatz von PKI bietet eine vertrauenswürdige Netzwerkumgebung, in der Kommunikation vor unberechtigtem Zugriff durch Verschlüsselung geschützt und die Authentizität des Kommunikationspartners durch die digitale Signatur gewährleistet ist. Die verschiedenen Anwendungen der PKI sind kryptografisch geschützt. Dazu gehören der Schutz von E-Mail-Anwendungen, von Desktopsystemen und von webbasierten Anwendungen, von E-Commerce, sowie die Zugriffskontrollen und die sichere Kommunikation in Virtual Private Networks (VPN).

Die PKI nutzt zwei Schlüssel mit einer typischen Länge von 1024 bis 2048 Bit. Einen privaten, den nur der Besitzer und die Zertifizierungsstelle kennen und der auch nie ausgelesen oder verschickt wird, sowie einen öffentlichen Schlüssel, der dem jeweiligen Geschäftspartner bekannt gemacht werden muss.

Die PKI-Architektur besteht aus den Instanzen Policy Certification Authority (PCA), Certification Authority (CA), Registration Authority (RA) und dem Zertifikatnehmer, die unterschiedliche Aufgaben realisieren. Darüber hinaus umfasst das PKI-Modell mehrere Funktionseinheiten wie das Key Management Center (KMC), die Time Stamping Authority (TSA) und das Key Recovery Center (KRC). Der ausgezeichnete Teil der PKI wird als Trust Center (TC) bezeichnet.

Eine Sicherheitsinfrastruktur muss für den Endbenutzer transparent sein, allerdings sollten die genauen Abläufe des Schlüssel- und Zertifikatmanagements vor dem Benutzer verborgen bleiben. Er sollte aber in der Lage sein, auf einfache Art und Weise die Services zu nutzen.

6. Aktuelles: Fall „ROCA“

Im Oktober 2017 wurde ein Fall bekannt, indem Chips der Firma Infinion eine erhebliche Sicherheitslücke aufweisen. Forscher fanden den Fehler, der vermutlich schon seit 2012 existiert, bereits Anfang des Jahresveröffentlicht wurde das ganze jedoch erst im Herbst.

Die Implementation des Chipherstellers ist dafür verantwortlich, die für das Schlüsselpaar notwendigen Primzahlen zu liefern. Durch einen Fehler liefert der Algorithmus in unregelmäßigen Abständen schlechte Primzahlen aus, die die kryptographische Stärke der erzeugten Schlüssel beeinträchtigen. 2048 bit RSA

Schlüssel können im Normalfall nicht im Zeitrahmen eines Menschenlebens geknackt werden. Durch den vorliegenden Angriff sind die betroffenen Schlüssel mittels Parallelisierung, schnell zu knacken.
Die Hersteller haben bereits Sicherheitspatches herausgegeben, die eingespielt wurden. Fest verbaute Chips, z.B. in 750.000 estnischen Personalausweisen, mussten jedoch vollständig ausgetauscht. Betroffen waren unter anderem Geräte der Hersteller Microsoft, Google, HP, Lenovo, Fujitsu, Yubi-Keys und Diverse Smartcards.

Literaturverzeichnis

[1] url: https://www.philipphauer.de/info/info/asymmetrische-verschluesselung/

[2] url: http://numbersandshapes.net/2012/04/the-chor-rivest-cryptosystem/

[3]url: https://www.elektronik-kompendium.de/sites/net/1910141.htm

[4] url: http://www.kryptowissen.de/asymmetrische-verschluesselung.html

[5] url: http://ddi.cs.uni-potsdam.de/Lehre/e-commerce/elBez2-5/page11 html.

[6] url: https://www.elektronik-kompendium.de/sites/net/1910111.htm

[7] url: https://www.elektronik-kompendium.de/sites/net/1910121.htm

[8] url: https://www.zum.de/Faecher/Inf/RP/infschul/kr_rsa.html#funktion

[9] url:

[10] url: http://www.elektronik-kompendium.de/sites/net/1910141.htm

[11] url: http://www.elektronik-kompendium.de/sites/net/0908071.htm

[12] url: https://www.heise.de/security/meldung/Sicherheitsforscher-an-AVHersteller-Finger-weg-von-HTTPS-3620159.html

[13] url: http://www.elektronik-kompendium.de/sites/net/1910131.htm

[14] url: http://www.itwissen.info/Digitale-Signatur-digital-signature-DSig.html

[15] url: http://www.itwissen.info/DSA-digital-signature-algorithm-DSAAlgorithmus. Html

[16] url: https://www.de.cgi.com/sites/default/files/files_de/factsheets/cybersecurity_roca_de.pdf

[17] url: https://www.elektronikpraxis.vogel.de/krypto-panne-bei-infineon-estland-zieht-elektronische-personalausweise-ein-a-660838/

[18] url: https://www.channelpartner.de/a/faq-was-sie-ueber-verschluesselung-wissen-sollten,3071779,3