LU06c - Digitale Signatur

Siehe http://de.wikipedia.org/wiki/Digitale_Signatur

Einleitung

Digitale Signaturen werden beim Versenden von Nachrichten wie z.B. eMail eingesetzt. Besonders im Geschäftsverkehr kann durch gefälschte eMails grosser Schaden angerichtet werden. Dabei ist das Fälschen von eMails relativ einfach:

- Angabe eines falschen Absenders.
- Verändern des Inhalts einer Nachricht während des Transports im Internet.

Um die Echtheit einer Nachricht zu bestätigen, wird die Nachricht mit einer digitalen Signatur versehen. Dabei werden zwei Ziele verfolgt:

- Ähnlich wie eine handschriftliche Unterschrift soll die digitale Signatur die Identität des Absenders einer Nachricht garantieren.
- Gleichzeitig bestätigt die digitale Signatur, dass der Inhalt der Nachricht nicht verändert wurde.

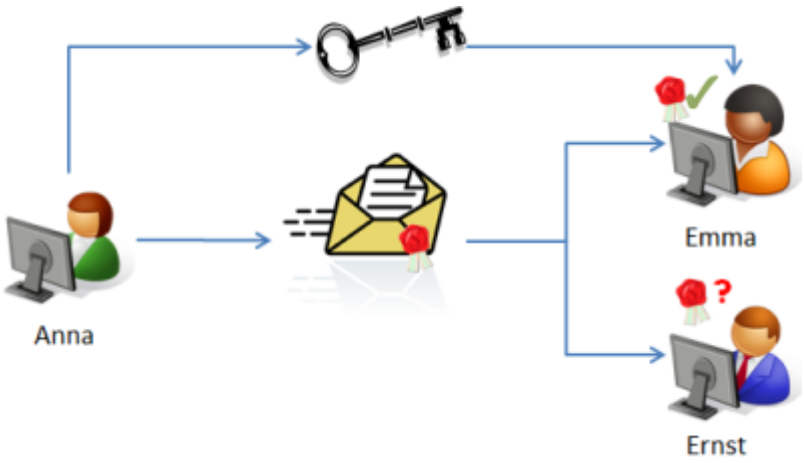
Anwendung

Die Signatur einer Nachricht basiert auf einem Verschlüsselungsverfahren mit zwei unterschiedlichen Schlüsseln.

- Ein geheimer Signaturschlüssel dient zum Signieren. Diesen Schlüssel darf nur der Absender kennen.
- Ein öffentlicher Verifikationsschlüssel dient zur Verifizierung der Signatur. Der Empfänger muss den Absender und dessen Verfikationsschlüssel kennen.

Ein solches Verfahren nennt man LU06d - Asymmetrisch Verschlüsseln.

Ablauf



In diesem Beispiel schickt Anna (Absender) eine wichtige Nachricht an Ernst und Emma (Empfänger). Das eMail-Programm von Anna und Emma verfügt über die notwendigen Funktionen um eMails zu signieren bzw. eine Signatur zu verifizieren.

1. Verifikationsschlüssel austauschen

Damit Emma die Signatur von Anna prüfen kann, benötigt Sie den Verifikationsschlüssel von Anna. Diesen Schlüssel kann Emma auf verschiedene Art erhalten:

- Anna sendet ein eMail mit dem Verfikationsschlüssel als Anhang.
- Anna stellt den Verifikationsschlüssel auf Ihre Homepage, wo Emma den Schlüssel kopieren kann.
- Anna übergibt Emma den Verifikationsschlüssel auf einem USB-Stick.

Emma speichert den Verifikationsschlüssel in ihrem eMail-Programm. In Zukunft kann das Programm die Signaturen von Anna verifizieren.

2. eMail verfassen

Anna muss beim Verfassen der eMail nichts besonderes beachten. Sie schreibt einfach ihren Text, hängt Dateien an und wählt die Empfänger Ernst und Emma aus.

3. eMail signieren

Bevor Anna die eMail abschickt, wählt sie die Option „Nachricht signieren“ in Ihrem eMail-Programm aus. Sobald Anna auf [Senden] klickt, signiert das eMail-Programm die Nachricht.

Beim Signieren einer Nachricht wird eine Reihe von Rechenoperationen ausgeführt. Basierend auf dem Signaturschlüssel und dem Inhalt der Nachricht wird ein Code generiert. Dieser Code wird mit der Nachricht als Anhang verschickt.

4. eMail empfangen und lesen

Ernst empfängt die eMail von Anna mit der Signatur im Anhang. Sein eMail-Programm kann aber nichts mit dieser Signatur anfangen. Daher weiss Ernst nicht, ob die Nachricht wirklich von Anna ist.

Natürlich könnte Ernst diese Signatur-Datei öffnen. Er würde dann sowas sehen:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.13 (Darwin)

mQENBEy2GCIBCACtCcloTPOZLq4kFDEqFjL+xI4xcc2DFsEt820GGtEeaZNDOlZd
LWWnW9TFWVByeN4+I/3V75ylTWfrhzvLSZ60ZUAvMAhGPoeHqRgAVaVQieLH+vW1
GNE5H4uQGIptuX5noD6IOSX/ZUy6YNlm1t0rhCNjiMQndIvFeSTwLxOiWfmY9HyW
9iRdiO6klYiU0ZK75STOXHqyslcmotICTOJw2tk1NyT1Vw18RtxwCx+MxzWlozQh
Dlx8aUc+hu9el2yz5JzX+5d/OHhAy+rGBnKuQZs3TEwUh5NaxOQblIkAEHGLkazC
BFDpNs0MzaJ1VHNJG8fMXiWPXltkExtkuiZFABEBAAG0JU1hcmt1cyBNZWllciA8
bWFya3VzLm1laWVyQGl0LmJ6ei5jaD6JATgEEwECACIFAlQlNb0CGwMGCwkIBwMC
BhUIAgkKCwQWAgMBAh4BAheAAAoJEBgNd7h0GfGyPOcIAIrLvDDZDe4AtyJMOJoL
tt5XDYlU4a7qui5NQ9CvcmlGTLnSD2ayCcIlqF9eeQZgViHomswNVlz5ZtgM2E9u
uXmdkrXlszr+ZAUX+K13U4jUbf9AHQuOWfsFAlC+C2/8t647iKEWxieZ3ierVpz+
s1HzxXE2XMSScACOhxp884RincaZLQR8VPd+S6acB9/Qhbhzqu+gGKmNWTXyEbvQ
8wb2JIxu9McvTtdYVMR2weJGAAuG2a2vXZ29Pltklypc74OV6OLNNGLijSNiLFXD
diVuMjOMk7toBdQejcHlYXG9+7EkGeugIzSuRn0F2XwVjE4wwYFclUPhGJv65Jsd
H9G0Ik1hcmt1cyBNZWllciA8bWFya3VzLm1laWVyQGJ6ei5jaD6JATgEEwECACIF
AlQlNa8CGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEBgNd7h0GfGy0rEH
/RJFPFfvMq7lqbL26qAJgOxC/JD9C3+MtQUiGoKKqRdZVluLaE4RacbUZz/CSvok
1jf11bl1IockQ/vWQSLpz/3shYcWO27bBOlByeq4ncpfCnwJRySCcNVKovoSZhX8
SI7npPM5xnzmdp9MlAmhomyHrnuya19YwFJ+zWpIrFS7r0waxx8CfXDVlxJLs/7D
X264OXso9zmZhgQchW+WDopuqUaT8xuTqc+XQnxeeAQLsj9R+uj5paKrHwQE49XW
rNvo2wbtrs28+gQnN8anq8/bJMBHQqN9KdQJH3fvvOSxPUEj5r1/U6GxDaT2tyu6
d+RgMB70tFBEFb7RN49RFOq0Hk1hcmt1cyBNZWllciA8bWFpbEBtMm1laWVyLmNo
PokBOAQTAQIAIgUCUoCdTQIbAwYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQ
GA13uHQZ8bKcpwgAjaCPYDR19hxZyTfi6sKeoRRnBuNLOqo9J3wGC0oV6pUztxJp
X5gzmKb6GEkYXAw1d0LkzGLZktAeYzDUdZnc1r8jWgPlCMLBejZM3Gm2MrhFZ1t7
4h1uIwkHI2cwFiVekvhfyAE0kZtj+soIJE3MZRdo7vS3KsqQ6Te89QT2mcrTwzvT
emGDTzK3fRMnr0xOixy6lW+bljcg4/4BJOcT7YYfwApmSAR/XTV2NAFPXOrK35b7
SX/xPxweRn9qpEbhQQ8J4fNnhNKT+LFnttwrnFsyto6u5qHV8W0Fpcvb/B27asWa
WPnaKicnsGqfrKI20Zj9I8hEVXQJNS2mSdzj/7QeTWFya3VzIE1laWVyIDxtMm1l
aWVyQGlubm8uY2g+iQE2BBMBAgAgBQJMthgiAhsDBgsJCAcDAgQVAggDBBYCAwEC
HgECF4AACgkQGA13uHQZ8bKXewf+I3WlJ+IMAOuEmcjXuW5PgmVSjKbvPXOd1d4D
O2eyxt524uK5/zMbB+u9R9foWyHrqNCTULcv1s/Ac+8GZAYveETGQ/NCiXz8RcXZ
hMHGAqEK/HP2f0wShpKeD+pqhKPINJsJPcQp24+ODRpKGw7f8MU+nhDMO0OrFak8
iTAIzY6E6euYUrYtzrugx+Eta7lpcsE3A92UV2wQoELVF1qENToS2cJ98foa2qJ5
EgS6yHOsVTqg/F+AR+LpniEkPwToDo/XLXtWlXckEG7C5XW976WIwJyZ2PqctQE0
XzR+Sa1Qx9sFb0O5khaIEMa4eCXIEbJ/3le4LGfRnDiVp+A3O7QoTWFya3VzIE1l
aWVyIDxtYXJrdXMubWVpZXJAc3R1ZC5waHpoLmNoPokBOAQTAQIAIgUCVCU1zgIb
AwYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQGA13uHQZ8bJSjQf/QJlpjeyF
g+kL5myQBkHHNrWB+z6xbxUeCat+kvpqnX0/TSUU89KFXh069z5iWq6oOnW9QKGR
2tHgboojWrDeup12Dxqjv8PjeXsmfGuF0n26tXjkbvJyVZuwTIa3MZVK1srwqtXp
mpWTbhrjmSFRjQ41gKqj5h3+WOQ2Zj5zN1E1Cw0vL2HqtiffgQW/WgVVUYmmtpCr
D3bS/G6XZlv5TkCw8t/f01rXPVFuVHFRXzL4ZurX6nfqyPG2I9YABvtPVUP8cpo+
CXQs4hG1ckqYKPJNx6dTKqxwaOu0gW2SHRnRMGm6R0YP0KawveVB4/0rvsrkY26O
OA6mss8HFsVVQLkBDQRMthgiAQgAxtgLb5CEUd1EnCj8mUsFu632ruEATTzbpk54
```

```
aOnsk7EOWC1xWgOSKXxjP7Ykec/oH5Wc+IvArb3+8s6MCGyDXGh89ECqE8Q9jJe8
y+LkAzewSbpaUAfq2LYw3MU7iMuvD8RQbDk9KxFvPboCIPRQDvLcAvZyRIw+WGjk
ZOjCn5JGxFoPkmPdrtAS8kjURqembMJylv39Iw2b9w6A9lwn1ynpZ7rEUQcypCry
gJoi7TC0y57sgdvY0LUkayIpHpTnbHQtb0TwRutPG67cUaGEOci4Bb2TX/l5McMX
0q0wo8E0gTohTaEsM9Tdsb49Ce+sOR6E7SJXiVS9S6LZuqPH8wARAQABiQEfBBgB
AgAJBQJMthgiAhsMAAoJEBgNd7h0GfGynVAH/1IiPWXckNxDSnxbVGLdwk+enQQN
l7vkWl6a/zc7CInC7SUDqpD8WiAFdVq6ZP6ZMxcFck+WyjxUxwDJ6iLD6vpA5V9b
3c7ZX3YYboeLadpfl8/lP7QJ7+Sy76Liy88l89jlgPOxqWt8n2C7KS8Lgjf1w8Lm
dQM3wMk49jPV0r1P5n/o0uyl8t97eNnQwPAOLUHas9zhs8nCLdarAilVmV3dxKyY
Tdgq2QXrqqcXW3UfKXLiXXeP1utGfYUAX7Zfs+lLy2s0NyilEg5w9sjv2YFHkcx0
saoeuWy2qUu/0YrvdH6GSpwdJLuOpIqC18YVqE4qyzNIrCf7XBa/9dc0wOc=
=SStK
-----END PGP PUBLIC KEY BLOCK-----
```

Emma empfängt die Nachricht ebenfalls. Ihr eMail-Programm erkennt die Signaturdatei und prüft nun den Absender und den Inhalt. Eine Information zeigt Emma an, ob die Nachricht wirklich von Anna stammt und ob der Inhalt unverändert ist.

Verfahren

Bei allen Verfahren zur digitalen Signatur ist gemeinsam, dass aus dem Signaturschlüssel und den Daten die Signatur berechnet wird. Dabei ist es wichtig, dass ...

- unterschiedliche Daten zu einer unterschiedlichen Signatur führen und
- unterschiedliche Schlüssel zu einer unterschiedlichen Signatur führen.

Dadurch soll es praktisch unmöglich sein, eine Signatur zu fälschen.

Wir werden die verschiedenen Verfahren anhand folgender Kriterien prüfen:

1. Authentizität
    - Nur der Absender kennt den Schlüssel und kann somit diese Signatur erstellen.
2. Integrität
    - Die Nachricht und die Signatur passen eindeutig zusammen ⇒ Die Nachricht entspricht dem Original.
3. Verifizierbarkeit
    - Der Empfänger kann prüfen, ob die Signatur vom Absender stammt..
4. Beweisbarkeit
    - Der Empfänger kann beweisen, dass die Signatur vom Absender stammt.

Manuelles Verfahren

Zum Verständnis versuchen wir, eine Nachricht mittels eines einfachen Verfahrens von Hand zu signieren.

Nachricht	Zum Verständnis versuchen wir, eine Nachricht mittels eines einfachen Verfahrens von Hand zu signieren.

Schlüssel	Der Schöppelimunggi u der Houderebäseler si einischt schpät am Abe, wo scho der Schibützu durs Gochlimoos pfoderet het, über s Batzmättere Heigisch im Erpfetli zueglüffe u hei nang na gschtigelet u gschigöggelet, das me z Gotts Bäri hätt chönne meine, si sige nanger scheich. [1)]

Nun benötigen wir noch eine Rechenvorschrift: Wir zählen für alle Buchstaben, wie oft sie im Text und dem Schlüssel vorkommen. Die Anzahl halten wir alphabetisch aufsteigend fest.

Signatur

- A = 11
- B = 6
- C = 16
- D = 9
- E = 47
- …

Der Empfänger führt das gleiche Verfahren durch, um die Echtheit der Nachricht zu prüfen.

Sicherheit

Prüfen wir dieses Verfahren anhand der Kriterien:

1. Authentizität 😕
   - Jeder Empfänger einer Nachricht muss den Schlüssel und das Verfahren kennen. Dadurch kann er in Zukunft Nachrichten im Namen des Absenders signieren.
2. Integrität 😕
   - Sie können den Inhalt der Nachricht durch umstellen der Wörter und Buchstaben verändern und erhalten noch immer die gleiche Signatur. Eine andere sinnvolle Nachricht mit den gleichen Buchstaben zu erstellen ist zwar schwierig, aber durchaus machbar.
3. Verifizierbarkeit 🙂
   - Der Absender kann seinen Schlüssel und das Verfahren veröffentlichen (z.B. auf seiner Homepage).
4. Beweisbarkeit 😕
   - Es lässt sich nicht beweisen, dass die Signatur wirklich vom Absender stammt (siehe Authentizität).

Hashwert

Bei Downloads im Internet wird auf einigen Seiten ein Hashwert der Daten angegeben. Dieser Hashwert wird aufgrund der binären Codierung der Daten berechnet. Man könnte dies mit dem Fingerabdruck eines Menschen vergleichen.

Somit kann der Hashwert als eine Art einfache Signatur betrachtet werden.

Am weitesten verbreitet sind

- MD5: 32 Byte langer Hashwert, veraltet.
- SHA-2: 40 Byte langer Hashwert.

Nachdem Sie die Daten heruntergeladen haben, vergleichen Sie den Hashwert der empfangenen Daten mit der Angabe im Internet. Sind beide Hashwerte identisch, so wurde der Download korrekt durchgeführt.

Die Rechenvorschriften für diese Hashverfahren sind standardisiert. Deshalb werden für die gleichen Daten unabhängig vom Absender die gleiche „Signatur“ erzeugt.

Hash mit Salt

Als Salt (deutsch: Salz) bezeichnet eine zufällig gewählte Zeichenfolge, die an die Daten angehängt wird. Der Hashwert wird durch das Anhängen des Salts grundlegend verändert, ähnlich wie sich der Geschmack von Essen durch hinzufügen von Salz verändert. Ohne Kenntnis des Salts ist es massiv schwieriger aus einem Hashwert die ursprünglichen Daten zu rekonstruieren.

Nur wenn der Empfänger der Daten das Salt kennt, kann er die Signatur prüfen.

Sicherheit

Prüfen wir dieses Verfahren anhand der Kriterien:

1. Authentizität 😕
   - Jeder Computer kann einen Hashwert berechnen. Somit lässt sich nicht prüfen, wer die Daten signiert hat.
2. Integrität 🙂
   - In Kombination mit einem Salt-Wert ist es sehr schwierig, mit veränderten Daten den gleichen Hashwert zu erzeugen.
3. Verifizierbarkeit 🙂
   - Das Verfahren ist allgemein bekannt. Der Absender kann sein Salt veröffentlichen (z.B. auf seiner Homepage).
4. Beweisbarkeit 😕
   - Es lässt sich nicht beweisen, dass die Signatur wirklich vom Absender stammt (siehe Authentizität).

Die Verwendung eines Hashwerts als Signatur funktioniert nur dann einigermassen zuverlässig, wenn genau zwei Personen Daten austauschen. Dazu dürfen aber nur diese zwei Personen das Salt kennen.

RSA-Signatur

Das bekannteste und am häufigsten eingesetzte Verfahren für digitale Signaturen ist RSA. Dieses Verfahren wurde nach seinen Entwicklern **R**ivest, **S**hamir und **A**dlemann, drei Mathematikern am MIT, benannt. Die Rechenvorschrift für RSA basiert auf einer Einwegfunktion mit einer Falltür.

Einwegfunktionen mit Falltür

Eine Einwegfunktion ist eine mathematische Funktion, die sich nur schwer in die andere Richtung berechnet werden kann. Die meisten mathematischen Funktionen lassen sich sehr einfach umkehren und sind daher für die Signatur ungeeignet. Zum Beispiel lässt sich die Addition „5 + 7 = 12“ sehr einfach in eine Subtraktion überführen: „12 - 5 = 7“.

Anders sieht es bei der Multiplikation aus. Es ist für Computer relativ einfach, eine zwei Zahlen zu multiplizieren: 12 * 8 = 96. Wesentlich aufwändiger ist es, eine Zahl in Ihre Faktoren zu zerlegen: 96 = x * y.

Falltür

Als Falltür bezeichnet man eine Information, welche das Umkehren der Berechnung vereinfacht. Eigentlich wäre der Begriff **Hintertür** wesentlich treffender.

Angenommen Sie wissen, dass die Zahl 3599 aus der Multiplikation von zwei Faktoren entstanden ist. Also x * y = 3599. Versuchen Sie einmal die beiden Faktoren zu ermitteln. Dazu müssen Sie viele verschiedene Kombinationen ausprobieren und würden vielleicht noch nicht einmal ein eindeutiges Ergebnis erhalten.

Ich verrate Ihnen nun die Falltür: x=59. Dadurch wird die Berechnung wieder sehr einfach.

Funktionsweise von RSA

Um Daten zu signieren, benötigen Sie einen öffentlichen und einen privaten Schlüssel.

- Der private Schlüssel besteht aus der Zahl zur Verschlüsselung (**e**) und dem RSA-Modul (**N**).
- Der öffentliche Schlüssel besteht aus der Zahl zur Entschlüsselung (**d**) und dem RSA-Modul (**N**).

Dabei wird sichergestellt, dass nur mit dem privaten Schlüssel die Signatur berechnet werden kann. Der öffentliche Schlüssel kann lediglich die Signatur entschlüsseln. Es ist ebenfalls unmöglich, aus dem öffentlichen Schlüssel den privaten Schlüssel zu berechnen. Sie können sich nicht vorstellen, dass dies möglich ist? Eine genaue Beschreibung und Begründung finden Sie im Kapitel RSA.

1. Anna berechnet den Hashwert ihrer Nachricht.
2. Anna verschlüsselt diesen Hashwert wird nun mit ihrem privaten Schlüssel. Dieser verschlüsselte Hashwert ist die Signatur der Nachricht.
3. Anschliessend schickt Anna die Nachricht als Klartext und die Signatur an Emma.
4. Emma berechnet den Hashwert der empfangenen Klartext-Nachricht.
5. Emma entschlüsselt die Signatur der Nachricht und erhält einen zweiten Hashwert.
6. Emma prüft nun, ob die beiden Hashwerte identisch sind.

Sicherheit

Prüfen wir dieses Verfahren anhand der Kriterien:

1. Authentizität 🙂
   - Nur wer den privaten Schlüssel kennt, kann die Signatur erstellen. Sofern der private Schlüssel nicht in fremde Hände gerät, ist die Authentizität gewährleistet.
2. Integrität 🙂
   - Es ist zwar möglich, eine gefälschte Nachricht mit einer gefälschten Signatur zu senden. Durch die angewandten Verfahren würde diese Nachricht aber keinen Sinn ergeben, wodurch der Empfänger den Betrugsversuch sofort erkennt.
3. Verifizierbarkeit 🙂
   - Der Absender kann seinen öffentlichen Schlüssel jedem zugänglich machen. Somit lässt sich die Herkunft einer Signatur recht gut prüfen.
4. Beweisbarkeit 🙂
   - Es lässt sich beweisen, dass die Signatur einer „sinnvollen“ Nachricht wirklich vom Absender stammt.

---

m114-A0G

[1)]

Dieser Text stammt aus „s'Totemügerli“ von Franz Hohler