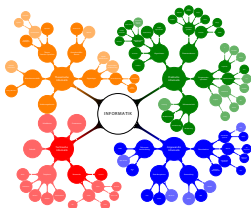


Kapitel 43

Kommunikations-Sicherheit

Verschlüsselung: Der digitale Briefumschlag

Vorlesung Einführung in die Informatik 2 vom 8. Juli 2014 von Till Tantau



Lernziele von Kapitel 43

1. Konzept der Verschlüsselung verstehen
2. Unterschied zwischen symmetrischen und asymmetrischen Verfahren kennen
3. Konzept der digitalen Unterschrift verstehen
4. Programme zur Verschlüsselung einsetzen können
5. Zertifikate erstellen und installieren können

Gliederung von Kapitel 43

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

43.2.1 Ziele

43.2.2 Symmetrische Verschlüsselung

43.2.3 Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

43.3.1 Vertraulichkeit: Digitale Briefumschläge

43.3.2 Authentizität: Digitale Unterschriften

43.3.3 Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

43.1 Ziele von IT-Sicherheit ◀

43.2 Verschlüsselung

Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften
Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

Bei *IT-Sicherheit* geht es um folgende Anliegen:

1. Schutz vor und die Aufrechterhaltung des Betriebs bei
 - ▶ Ausfall von Teilen des Systems (Stromausfall, Absturz)
 - ▶ Angriffen auf das System (durch Hacker, korruptierte Mitarbeiter)

Diese *Systemsicherheit* wird uns im nächsten Kapitel interessieren.

2. Schutz von Daten und Kommunikation vor
 - ▶ Spionage
 - ▶ Fälschung

Diese *Daten- und Kommunikationssicherheit* wird uns in diesem Kapitel interessieren.

Ziele der Verschlüsselung von Daten und Kommunikation

Kapitel 43 Kommunikations- Sicherheit

Vertraulichkeit Es muss sichergestellt werden, dass Daten und Kommunikation nur von »den Guten« gelesen werden können.
(Meine Daten gehen niemand etwas an.)

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

- Ziele
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale Briefumschläge
Authentizität: Digitale Unterschriften
Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

Integrität Es muss sichergestellt werden, dass Daten und Kommunikation nicht verfälscht werden können.
(Aus 1000 Euro dürfen nicht 10000 Euro werden.)

Authentizität Es muss sichergestellt werden, dass Daten und Kommunikation wirklich von den behaupteten Personen stammen.
(Die Email mit Alices Absenderadresse wurde tatsächlich von Alice versandt;
der Online-Banking-Server muss wirklich der Server meiner Bank sein.)

43-5

Zur Übung

Beurteilen Sie Postkarten, versiegelte Briefe und die Eröffnung eines Bankkontos bei einer Online-Bank in Bezug auf die drei Kriterien.

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale Briefumschläge
Authentizität: Digitale Unterschriften
Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

- Zum Schutz vor unbefugtem Lesen kann man Daten und Kommunikation *verschlüsseln*.
Dazu benutzt man ein *Verschlüsselungsverfahren* sowie einen *geheimen Schlüssel*.
- Beim *Verschlüsseln* (encryption) wird ein *Klartext* m (message) zusammen mit dem *Schlüssel* k (key) in ein *Chiffretext* $c = e(m, k)$ verwandelt.
Dies entspricht dem »Abschließen« mit dem Schlüssel.
- Beim *Entschlüsseln* (decryption) wird der Chiffretext zusammen mit dem Schlüssel in den Klartext zurückverwandelt, d.h. $m = d(c, k)$.
Dies entspricht dem »Aufschließen« mit dem Schlüssel.
- Da man zum »Auf- und Zuschließen« denselben Schlüssel verwendet, spricht man von *symmetrischen Verfahren*.

- ▶ Bereits in der Antike nutzte Julius Cäsar Verschlüsselungen, wenn er Befehle an seine Feldherren übermittelte.
- ▶ Das als *Cäsar-Chiffre* bekannte Verfahren funktioniert wie folgt: Jeder Buchstabe der Nachricht wird durch den Buchstaben ersetzt, der *drei Buchstaben später im Alphabet* kommt.
- ▶ Allgemeiner kann man statt »drei Buchstaben später« auch » k Buchstaben später« benutzen.
- ▶ Mathematisch ist also e die Funktion, die eine Nachricht und eine Zahl k nimmt und jeden Buchstaben der Nachricht um k viele Stellen im Alphabet vorwärts schiebt. Entsprechend schiebt d jeden Buchstaben um k viele Stellen zurück.

Zur Diskussion

Betätigen Sie sich als *Kryptoanalytiker*! Wie kann man – ohne Kenntnis des Schlüssels k – eine mit einer Cäsar-Chiffre kodierte Nachricht entschlüsseln?

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

- ▶ Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale Briefumschläge
Authentizität: Digitale Unterschriften
Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

Beispiel einer Cäsar-Verschlüsselung

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale Briefumschläge
Authentizität: Digitale Unterschriften
Echtheits-Zertifikate: Digitale Notare

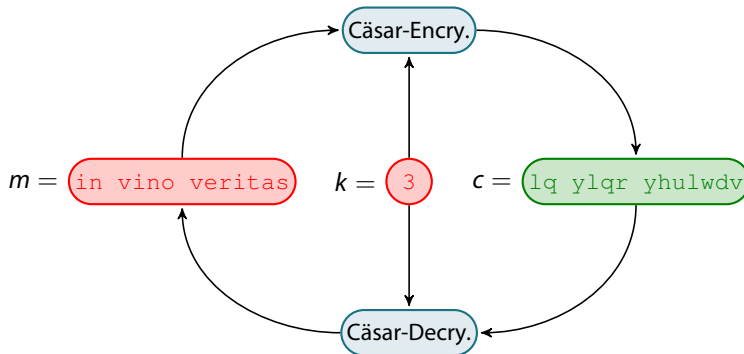
43.4 Sicheres Surfen

43-8

Rot = geheim, Grün = öffentlich



Public domain



Da die Cäsar-Chiffre offenbar nicht sonderlich sicher ist, benötigen wir ein besseres Verfahren:

One-Time-Pad-Algorithmus (Ver- und Entschlüsselung)

Eingaben seien die Nachricht m und der Schlüssel k *gleicher Länge*

1. Schreibe Nachricht und Schlüssel als Bitstrings auf (wie im ersten Kapitel).
 2. Bilde nun das bitweise XOR von Nachricht und Schlüssel. Dies bedeutet: Flippe das i -te Bit der Nachricht, wenn das i -te Bit des Schlüssels eine 1 ist.
- ▶ Wie der Name schon sagt, kann man das Verfahren leider nur einmal pro Schlüssel (sicher) verwenden.
 - ▶ Außerdem sind die Schlüssel schrecklich lang.

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

- ▶ Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

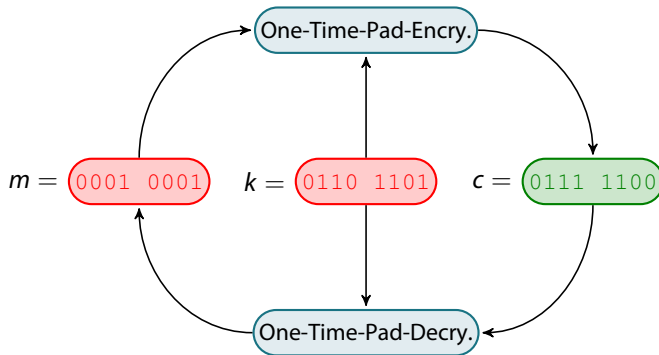
43.3 Sichere E-Mail

Vertraulichkeit: Digitale Briefumschläge
Authentizität: Digitale Unterschriften
Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

Beispiel einer One-Time-Pad-Verschlüsselung

Rot = geheim, Grün = öffentlich



43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale Briefumschläge
Authentizität: Digitale Unterschriften
Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale Briefumschläge
Authentizität: Digitale Unterschriften
Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

- Moderne symmetrische Verschlüsselungsverfahren kann man sich als eine *sehr clevere Mischung* aus Cäsar-Verfahren und One-Time-Pad vorstellen.
- Lange Zeit war das amerikanische DES (data encryption standard) das wichtigste Verfahren. Wegen Problemen wie Ausfuhrverbot, zu kurze Schlüssellänge und Patenten wurde es vor gut 10 Jahren durch ein moderneres und sicheres Verfahren ersetzt.
- Der neue internationale Standard nennt sich AES (advanced encryption standard).

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale Briefumschläge
Authentizität: Digitale Unterschriften
Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

Wann ist ein Verfahren »sicher«?

- *Informationstheoretisch sicher* heißt ein Verfahren, wenn man Chiffretexte ohne Kenntnis des Schlüssels nicht entschlüsseln kann.
- Leider kann man zeigen, dass nur One-Time-Pad-Verfahren in diesem Sinn sicher sind.
- *Komplexitätstheoretisch sicher* heißt ein Verfahren, wenn es für die Entschlüsselung kein wesentlich schnelleres Verfahren gibt, als alle Schlüssel durchzuprobieren.
- Bei Schlüssellängen ab 500 Bits ist solch eine Sicherheitsstufe dann *in diesem Universum nicht zu brechen*.

Eine ungewöhnliche Idee.

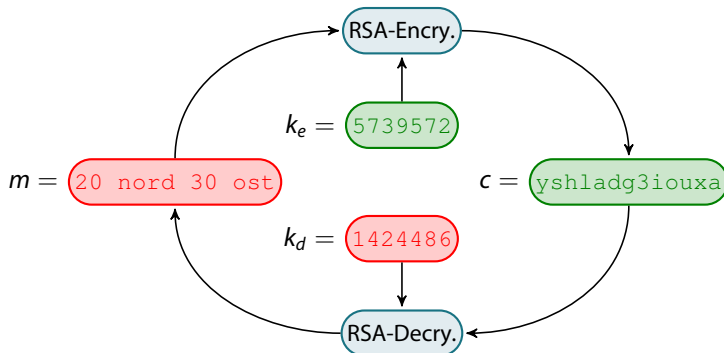
- ▶ Symmetrische Verschlüsselungsverfahren haben den *Nachteil*, dass Kommunikationspartner erstmal einen *Schlüssel sicher austauschen müssen*.
- ▶ Rivest, Shamir und Adleman haben 1977 ein Verfahren vorgeschlagen, *bei dem man keinen Schlüssel auszutauschen braucht* – das RSA-Verfahren. (Es gab vorher auch schon ein schlechteres, geheimgehaltenes Verfahren.)
- ▶ Heute ist dies ein Spezialfall der *Klasse der asymmetrischen Verschlüsselungsverfahren*.

Idee der asymmetrischen Verfahren

- ▶ Man benutzt *zwei Schlüssel*.
- ▶ Wenn man eine Nachricht mit einem ersten Schlüssel »abschließt«, kann man sie *nur mit dem zweiten Schlüssel »aufschließen«*.
- ▶ Kennt man einen der Schlüssel, so kann man daraus nicht mit vertretbarem Aufwand den anderen Schlüssel generieren.

Ablauf einer asymmetrischen Verschlüsselung.

- Die Royal Airforce möchte den Aufenthaltsort von Prinz Harry an den Buckingham Palace schicken.
- Dazu braucht sie nur den *öffentlichen Schlüssel 5739572 des Buckingham Palace* zu kennen.
- Nur im Palast kennt man den *privaten Schlüssel 1424486 des Palastes* und kann die Nachricht entschlüsseln.



43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung

► Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften
Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

Eine Nachricht soll vertraulich sein.

Ziel: Vertraulichkeit

- Eine Nachricht soll einer Person zugestellt werden.
- Nur diese Person soll die Nachricht lesen können.

Dies nennt man auch einen *digitalen Briefumschlag*.

Methode

- Die Person erzeugt ein RSA-Paar (k_e, k_d) .
- Der Schlüssel k_e wird »allgemein bekanntgegeben« und heißt nun *öffentlicher Schlüssel*.
- Nachrichten werden mit dem öffentlichen Schlüssel der Person verschlüsselt.
- Effekt: Nur diese Person kann die Nachricht (mit dem nur ihr bekannten privaten Schlüssel k_d) entschlüsseln.

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung

Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

- Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

- Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

- Zur Erzeugung eines Schlüsselpaares benutzt man ein *geeignetes Programm* wie beispielsweise `openssl`.
- Bei MacOS kann man auch komfortabel den *Schlüsselbundverwaltung* nutzen.

(Das Verfahren wird gleich noch etwas komplizierter werden, aber kümmern wir uns erstmal um den einfachen Fall.)

Praktische Umsetzung: Erzeugen des Schlüsselpaares.

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

- Ziele
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

- Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

Zertifikatsassistent

Eigenes Zertifikat erstellen

Legen Sie einen Namen für Ihr Zertifikat fest:

Sie sind im Begriff, ein sicheres E-Mail-Zertifikat zu erstellen (S/MIME). Das erstellte Schlüsselpaar verwendet 2048-Bit RSA. Wenn Sie diese Standardwerte ändern möchten, klicken Sie auf „Standardwerte überschreiben“.

Name:

Typ:

☐ Standardwerte überschreiben
(Legen Sie z. B. Erweiterungen, Zielschlüsselbund usw. fest)

Screenshot by Till Tantau

Praktische Umsetzung: Erzeugen des Schlüsselpaares.

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

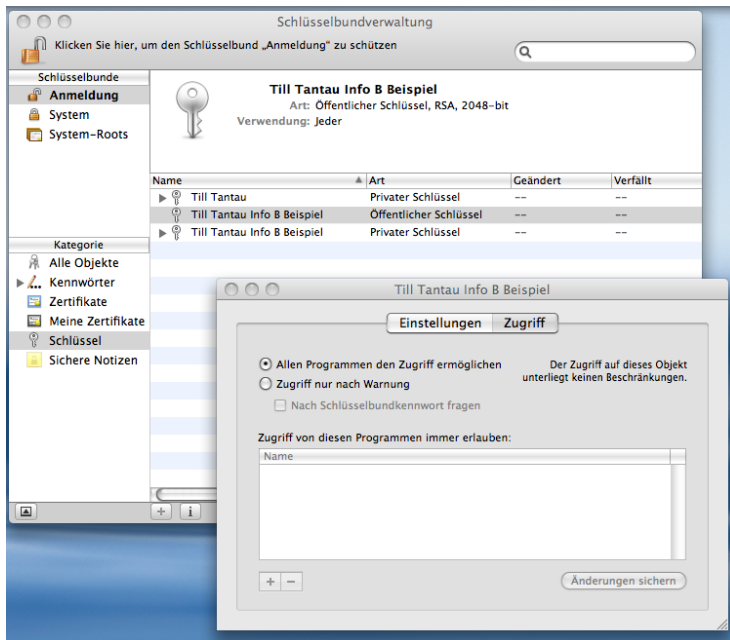
Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

- ▶ Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

43-16



Praktische Umsetzung: Erzeugen des Schlüsselpaares.

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

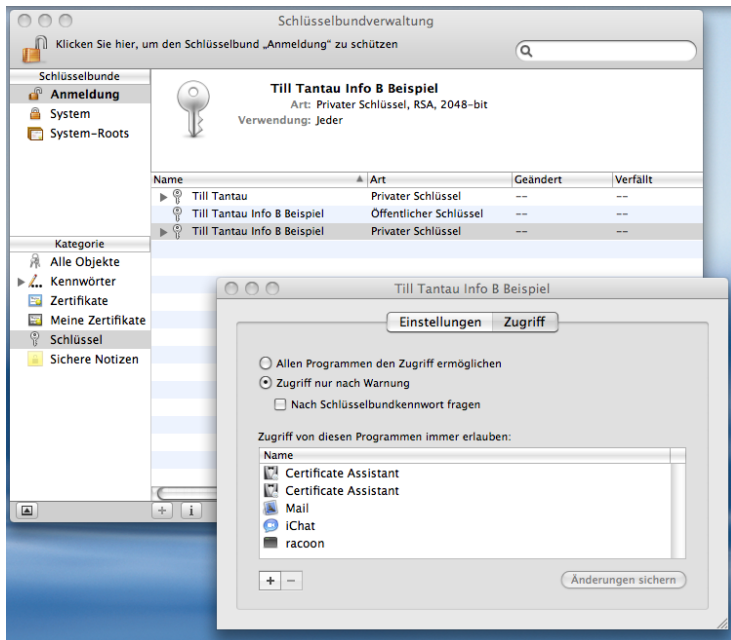
Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

- ▶ Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

43-16



Praktische Umsetzung: E-Mail an Johannes.

Schritt 1: Wir brauchen Johannes öffentlichen Schlüssel.

- ▶ Um eine Mail zu verschlüsseln, muss das E-Mail-Programm den *öffentlichen Schlüssel der Person kennen, der man eine E-Mail schreiben möchte*.
- ▶ Diesen öffentlichen Schlüssel kann einem die Person beispielsweise vorher geschickt haben.
- ▶ E-Mail-Programme oder die Schlüsselverwaltung erlaubt es, solche öffentliche Schlüssel zu *importieren* (ein geeigneter Menüpunkt).

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

- ▶ Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

Praktische Umsetzung: E-Mail an Johannes.

Schritt 1: Wir brauchen Johannes öffentlichen Schlüssel.

So sieht der öffentliche Schlüssel von Johannes beispielsweise wie folgt aus:

```
-----BEGIN CERTIFICATE-----
MIIFSTCCBDGgAwIBAgIECz1arTANBgkqhkiG9w0BAQUFADCBgqzELMAkGA1UEBhMC
REUxIDAeBgNVBAoTF1VuaXZlc3NpdGFldCB6dSBMdWVlZWNRMS4wLAYDVQQLEyVJ
bnN0aXRldCBmdWVyeIE1lZG16aW5pc2NoZSBjb2Vzcm1hdGlrMScwJQYDVQQDEx5D
QSBkZXIgwVW5pdmVyc2l0YWV0IHplIEEx1ZWJlY2sxITAfBgkqhkiG9w0BCQEWEnBr
aUB1bmktbHVlYmVjay5kZTAeFw0wNzEwMjEwMTM4MDdaFw0xMDEwMjEwMTM4MDda
... 20 ausgelassene Zeilen ...
Q8RGGPHGKcAocX3kGB3VTWZptDCACiJ9E5Q5pD4mWMPYAgYn jJwVv4KzF5Moboe
29IKgSvifr5ttcdqCFn5gfwVYrHWOLxxSZkbUpqGIIsAhoGeWd65Z9u4FARi87UIw
3KCso+ohahGUeVqZQk6ZXU6zJX/hw6K4y21lQfiBwVQuNjvudADM3Q6RSedECK4m
MsUhRqoUqvXegCZ7mA==
-----END CERTIFICATE-----
```

► Er kann auf

<https://pki.pca.dfn.de/uzl-ca/cgi-bin/pub/pki>
heruntergeladen werden.

► Alternativ kann Johannes den Schlüssel zunächst von seinem Mail-Programm oder von der Schlüsselverwaltung *exportieren* und dann verschicken (zur Not per Post).

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

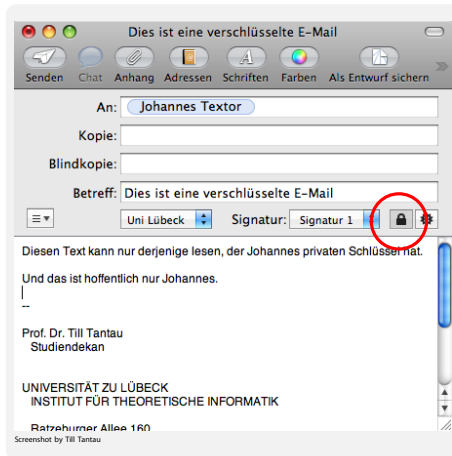
- Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

Praktische Umsetzung: E-Mail an Johannes.

Schritt 2: Schreiben und abschicken der E-Mail.

- ▶ Hat man dem eigenen System erstmal Johannes öffentlichen Schlüssel beigebracht, so kann man ihm eine verschlüsselte E-Mail schreiben.
- ▶ Bei modernen E-Mail-Programmen muss man dazu einfach auf einen Verschlüsselungsknopf drücken.



Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

- Ziele
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

- ▶ Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

43-18

Praktische Umsetzung: E-Mail an Johannes.

Schritt 2: Schreiben und abschicken der E-Mail.

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung

Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

- Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

- An Johannes wird dann ein mit dem *öffentlichen Schlüssel von Johannes verschlüsselter* Text geschickt.
- Um den Text zu entschlüsseln, braucht man den privaten Schlüssel von Johannes.
- Folglich kann niemand außer Johannes – *nichtmal der Autor der Mail* – den Text wieder entschlüsseln.

Praktische Umsetzung: E-Mail an Johannes.

Schritt 2: Schreiben und abschicken der E-Mail.

Message-Id: <AF944753-2276-487B-9BB1-995DA5D2058F@tcs.uni-luebeck.de>
From: Till Tantau <tautau@tcs.uni-luebeck.de>
To: Johannes Textor <textor@tcs.uni-luebeck.de>
Content-Type: application/pkcs7-mime;
name=smime.p7m;
smime-type=enveloped-data
Content-Transfer-Encoding: base64
X-Smtp-Server: theogate.tcs.uni-luebeck.de:tautau
Content-Disposition: attachment;
filename=smime.p7m
Mime-Version: 1.0 (Apple Message framework v936)
Subject: =?ISO-8859-1?Q?Dies_ist_eine_verschl=FCsselte_E-Mail?=
Date: Fri, 11 Jun 2010 16:05:31 +0200

MIAGCSqGSIB3DQEHA6CAMIACAQAxggoiMIIBzQIBADCbtDCBqzELMAKGA1UEBhMCREUxIDAeBgNV
BAoTF1VuaXZlcnpdGF1dCB6dSBmdWViZWNRMS4wLAYDVQQLZyVJbnN0aXRldCBmdWVyeIE1lZG16
aW5pc2NoZSBjb2Vzcm1hdGlrMScwJQYDVQDEx5DQSBkZXIgwV5pdmVyc210YWV0IHplIE1lZG16
Y2sxITAfBgkqhkiG9w0BCQEWEnBraUblbmktbHVlYmVjay5kZQIECz1arTANBgkqhkiG9w0BAQEF
AASCAQDbXGgvqKCcu+QdlxfTLsJKW6I8T2Eds7kslqtVBVoD6RFzcHF7XOT1lzcOmxcG2GS8frzNr
pVIC5VBssy/BEnm3BCpD8sw8HCxE0pcIm96/p5oHp9Qyk0FYs97JF3GLHVXPas8AoHEMoVBXAuku
... 66 ausgelassene Zeilen ...
FbiGph3to8Q/xaLEGHplQNN245YGcAY3xPAKibQfs3725ctGA9bBUX1iZneJMXR15DMWcd8VozAA
3MAQYwRiFuprLx7pYUMEbSUN12dq14WhTYS+6MvVEbj5ItZ68PWDx2OFsqm5enq158XViNLuS58
aTzsJ6uw861gEgqbbiD8wpMEzXpBCBx07+jmfobYe16/gFjInEB7XOV+VC95GEryi87pu3GAQI
qJB1HZWcdHQAAAAAAAAAAAAA

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

- Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

- Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

- Generell gilt: Ihr *privater* Schlüssel ist nur Ihnen bekannt (auch nicht Ihrem Lover!) und möglichst gut auf Ihrem Computer geschützt.
 - Am sichersten ist es, wenn der Schlüssel auf einer separaten Karte liegt, die ihrerseits durch eine PIN geschützt ist – dies ist mit dem neuen Personalausweis möglich.
 - In der Praxis liegt Ihr privater Schlüssel aber auf Ihrer Festplatte.
 - Dort ist er selbst wieder durch ein Master-Passwort symmetrisch verschlüsselt und damit selbst vor Diebstahl des Computers oder vor böartigen Hackern geschützt.
- Generell gilt: *Öffentliche* Schlüssel sind möglichst breit gestreut und überall verfügbar. Sie sollten auf Ihrem System die öffentlichen Schlüssel aller Ihnen bekannter Personen haben.

Zusammenfassung: Wer bekommt welchen Schlüssel?

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

- Ziele
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

- Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

43-19

Schlüsselbundverwaltung

Klicken Sie hier, um den Schlüsselbund „Anmeldung“ zu schützen

Schlüsselbunde

- Anmeldung
- System
- System-Roots

Kategorie

- Alle Objekte
- Kennwörter
- Zertifikate**
- Meine Zertifikate
- Schlüssel
- Sichere Notizen

Johannes Christian Textor

Ausgestellt von: CA der Universitaet zu Luebeck
Gültig bis: Freitag, 22. Oktober 2010 13:38 Uhr MESZ
✓ Dieses Zertifikat ist gültig.

Name	Art	Verfällt
Axel Wegener	Zertifikat	30.06.2011 00:00:00
CA der Universitaet zu Luebeck	Zertifikat	14.03.2019 00:00:00
Christian Kier	Zertifikat	22.01.2011 00:00:00
Claudia Anna Catharina Mamat	Zertifikat	22.10.2010 00:00:00
Deutsche Telekom Root CA 2	Zertifikat	10.07.2019 00:00:00
DFN-Verein PCA Global - G01	Zertifikat	01.07.2019 00:00:00
Dr. Christoph Reinecke	Zertifikat	20.08.2012 00:00:00
Hartmut Suefke	Zertifikat	05.10.2012 00:00:00
Helge Illig	Zertifikat	11.08.2012 00:00:00
Johannes Christian Textor	Zertifikat	22.10.2010 00:00:00
Madlen Kayserling	Zertifikat	02.02.2013 00:00:00
mail.gmx.net	Zertifikat	17.11.2011 00:00:00
Michael Elberfeld	Zertifikat	24.10.2010 00:00:00

24 Objekte

Screenshot by Till Tantau

Eine Nachricht soll digital unterschrieben werden.

Ziel: Authentizität

Es soll garantiert werden, dass eine Nachricht von einer bestimmten Person stammt.

Dies nennt man auch eine *digitale Unterschrift*.

Methode

Man benutzt dieselben Schlüssel wie beim Verschlüsseln von Nachrichten, *nur umgekehrt*:

- Die zu unterschreibende Nachricht wird mit dem *privaten Schlüssel* k_e verschlüsselt und dieser Text an die Originalnachricht angehängt.
- Überprüfung: Man entschlüsselt den verschlüsselten Teil mit dem öffentlichen Schlüssel k_d und vergleicht ihn mit dem behaupteten Text.
- Effekt: Nur die Person, die k_e kennt, kann die unterschriebene Nachricht erzeugen.

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung

Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge

► Authentizität: Digitale
Unterschriften

Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

Ablauf einer digitalen Unterschrift.

43.1 Ziele von IT-Sicherheit

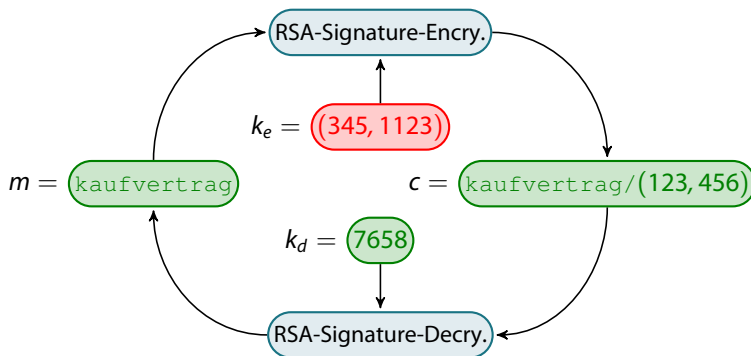
43.2 Verschlüsselung

Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

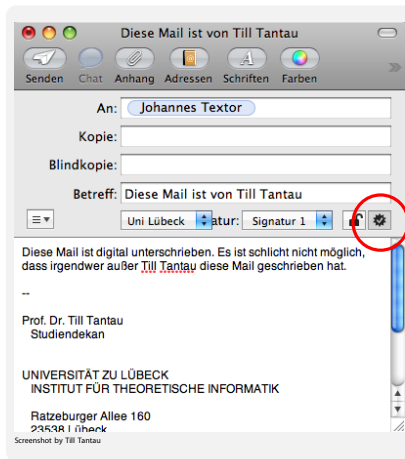
Vertraulichkeit: Digitale
Briefumschläge
► Authentizität: Digitale
Unterschriften
Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen



Praktische Umsetzung: Unterschriebene E-Mail an Johannes.

- Um eine E-Mail zu unterschreiben, braucht man lediglich den eigenen privaten Schlüssel – und den haben wir ja schon erzeugt.
- Damit jemand die E-Mail überprüfen kann, braucht er den öffentlichen Schlüssel – diese sind ja aber frei zugänglich.



Achtung: Mit »Signatur« wird auch manchmal der Standard-Text am Ende einer Mail bezeichnet.
Dieser ist *keine* digitale Unterschrift.

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

- Ziele
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

- Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

Praktische Umsetzung: Unterschriebene E-Mail an Johannes.

Kapitel 43 Kommunikations- Sicherheit

```
Message-Id: <A15605B5-9389-442D-BD9E-FC65D76A18DD@tcs.uni-luebeck.de>
From: Till Tantau <tantau@tcs.uni-luebeck.de>
To: Johannes Textor <textor@tcs.uni-luebeck.de>
Content-Type: multipart/signed;
boundary=Apple-Mail-11--309560619;
micalg=shal;
protocol="application/pkcs7-signature"
X-Smtp-Server: theogate.tcs.uni-luebeck.de:tantau
Mime-Version: 1.0 (Apple Message framework v936)
Subject: Diese Mail ist von Till Tantau
Date: Mon, 14 Jun 2010 08:44:26 +0200
```

... 13 ausgelassene Zeilen ...

Diese Mail ist digital unterschrieben. Es ist schlicht nicht möglich, =20=

dass irgendwer außer Till Tantau diese Mail geschrieben hat.

... 62 ausgelassene Zeilen ...

```
--Apple-Mail-11--309560619
Content-Disposition: attachment;
filename=smime.p7s
Content-Type: application/pkcs7-signature;
name=smime.p7s
Content-Transfer-Encoding: base64
```

```
MIAGCSqGSIB3DQEHAQcAMIAQAQExCzAJBgUrDgMCGGUAMIAGCSqGSIB3DQEHAQAAoIIOnzCCBCEW
ggMJoAMCAQICAgDHMA0GCSqGSIB3DQEBBQUAMHExCzAJBgNVBAYTAkRFRMRwGgYDVQQKEExNE2XV0
c2NoZSBUZwXla29tIEFHMR8wHQYDVQQLZXZULVR1bGVTV2WmGVHJlc3QgQ2VudGVyMSMwIQYDVQQD
... 79 ausgelassene Zeilen ...
DfPFZundteQqc6R/FdbTj67j23Y5h/8+qCIewT//LLWh4hvW/kEs7b1lIbcm3yniFd4PzjkKI9gi
WuPJkqz3VrcuYgfjCHT3RGyAANNQOF6fiJQ5tipmN4dHkfoxWQ7nPBobS13MLLd+fIvBrI78pTp
8mFDaOsObxdlyOXhm5RTBor2U/4uDGtZJddGOCNLPnJnCqEti3PWAHD/IAAAAAAAAA==
```

```
--Apple-Mail-11--309560619--
```

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge
► Authentizität: Digitale
Unterschriften
Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften

- Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

- Damit ich Johannes eine sichere Mail schreiben kann, muss er mir seinen öffentlichen Schlüssel zukommen lassen.
- Nun könnte auch irgendjemand anderes mir einen Schlüssel schicken und behaupten, er sei Johannes und dies sei sein Schlüssel.
- Um das auszuschließen, würde ich gerne verlangen, dass die Mail von Johannes unterschrieben ist – aber dazu brauche ich ja gerade den öffentlichen Schlüssel, um den es gerade geht.

Certificate-Authorities zertifizieren die Echtheit von Schlüsseln.

Ziel: Echtheit von Schlüsseln bezeugen

A will sichergehen, dass ein vermeintlicher öffentliche Schlüssel von B tatsächlich von B stammt.

Methode

- ▶ Eine *vertrauenswürdige Instanz*, »Certificate Authority (CA)« oder »Trust-Center« genannt, legt *Root-Schlüssel* (k_d , k_e) für digitale Unterschriften an.
- ▶ Der öffentliche Schlüssel k_d ist allgemein bekannt (er ist zum Beispiel in Ihren Browser schon fest eingebaut).
- ▶ Benutzer B lässt sich von der vertrauenswürdigen Instanz den folgenden Text unterschreiben: »Person B hat den öffentlichen Schlüssel 1234567.«
- ▶ Wenn A mit B zum ersten Mal redet, schickt B diesen unterschriebenen Text.
- ▶ A kann die Unterschrift der CA überprüfen (A kennt ja das Root-Zertifikat) und kann dann den öffentlichen Schlüssel von B benutzen.

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung

Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge

Authentizität: Digitale
Unterschriften

▶ Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

Certificate-Authorities zertifizieren die Echtheit von Schlüsseln.

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften
► Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

- ▶ Die privaten Schlüssel der Root-CAs sind *extrem gut gesichert*.
- ▶ Das darf man sich in etwa wie bei Mission Impossible vorstellen – inklusive gepanzerter Räume mit Servern, die vom Netz und auch von sonst allem getrennt sind.
- ▶ Selbst wenn Sie mit Ihrer Privatarmee das Gebäude stürmen, die wackeren Systemadministratoren überwältigen bevor diese die Schlüssel löschen können und den Schlüssel stehlen, würde das nicht viel nützen.
- ▶ Schlüssel können in zentralen Verzeichnissen als ungültig erklärt werden, was einige Minuten nach Ihrem Angriff der Fall wäre.
- ▶ Merke: Wenn man den privaten Schlüssel einer Root-CA klaut, so darf dies niemand merken. Ich empfehle, sich beispielsweise an Herrn Hunt zu wenden.

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften


- Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

- In der Praxis kann die Root-CA nicht die Schlüssel beispielsweise aller Deutschen unterschreiben.
- Stattdessen gibt es »Zwischen-CAs«.

Kaskaden von Unterschriften

Johannes Christian Textor

 **Johannes Christian Textor**
Ausgestellt von: CA der Universitaet zu Luebeck
Gültig bis: Freitag, 22. Oktober 2010 13:38 Uhr MESZ
Dieses Zertifikat ist gültig.

► Vertrauen
▼ Details

Name des Inhabers

Ländername	DE
Organisation	Universitaet zu Luebeck
Organisationseinheit	ITCS
Allgemeiner Name	Johannes Christian Textor

Name des Ausstellers

Ländername	DE
Organisation	Universitaet zu Luebeck
Organisationseinheit	Institut fuer Medizinische Informatik
Allgemeiner Name	CA der Universitaet zu Luebeck
E-Mail-Adresse	pki@uni-luebeck.de

Seriennummer 188570285
Version 3

Signaturalgorithmus SHA-1 mit RSA-Verschlüsselung (1 2 840 113549 1 1 5)
Parameter Ohne

Erst gültig ab Dienstag, 23. Oktober 2007 13:38 Uhr MESZ
Nur gültig bis Freitag, 22. Oktober 2010 13:38 Uhr MESZ

Öffentlicher Schlüssel

Algorithmus	RSA-Verschlüsselung (1 2 840 113549 1 1 1)
Parameter	Ohne
Öffentlicher Schlüssel	256 Byte : FC F4 E2 A5 BC 35 45 08 ...
Exponent	65537
Schlüssellänge	2048 Bit
Schlüsselverwendung	Verschlüsseln, Überprüfen, Einpacken, Ableiten

Screenshot by Till Tantau

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail


Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften
► Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

43-25

Kaskaden von Unterschriften

CA der Universitaet zu Luebeck

 **CA der Universitaet zu Luebeck**
Zwischenzertifizierungs-Instanz
Gültig bis: Donnerstag, 14. März 2019 1:00 Uhr MEZ
Dieses Zertifikat ist gültig.

► Vertrauen
▼ Details

Name des Inhabers

Ländername DE
Organisation Universitaet zu Luebeck
Organisationseinheit Institut fuer Medizinische Informatik
Allgemeiner Name CA der Universitaet zu Luebeck
E-Mail-Adresse pki@uni-luebeck.de

Name des Ausstellers

Ländername DE
Organisation DFN-Verein
Organisationseinheit DFN-PKI
Allgemeiner Name DFN-Verein PCA Global - G01

Seriennummer 169379686
Version 3

Signaturalgorithmus SHA-1 mit RSA-Verschlüsselung (1 2 840 113549 1 1 5)
Parameter Ohne

Erst gültig ab Donnerstag, 15. März 2007 9:54 Uhr MEZ
Nur gültig bis Donnerstag, 14. März 2019 1:00 Uhr MEZ

Öffentlicher Schlüssel

Algorithmus RSA-Verschlüsselung (1 2 840 113549 1 1 1)
Parameter Ohne

Öffentlicher Schlüssel 256 Byte : 96 65 2E E6 AF B5 E3 8F ...
Exponent 65537
Schlüssellänge 2048 Bit
Schlüsselverwendung Überprüfen

Screenshot by Till Tantau

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail


Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften
► Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

43-25

Kaskaden von Unterschriften

DFN-Verein PCA Global – G01

 **DFN-Verein PCA Global – G01**
Zwischenzertifizierungs-Instanz
Gültig bis: Montag, 1. Juli 2019 1:59 Uhr MESZ
✔ Dieses Zertifikat ist gültig.

► Vertrauen
▼ Details

Name des Inhabers	
Ländername	DE
Organisation	DFN-Verein
Organisationseinheit	DFN-PKI
Allgemeiner Name	DFN-Verein PCA Global – G01
Name des Ausstellers	
Ländername	DE
Organisation	Deutsche Telekom AG
Organisationseinheit	T-TeleSec Trust Center
Allgemeiner Name	Deutsche Telekom Root CA 2
Seriennummer	199
Version	3
Signaturalgorithmus	SHA-1 mit RSA-Verschlüsselung (1 2 840 113549 1 1 5)
Parameter	Ohne
Erst gültig ab	Dienstag, 19. Dezember 2006 11:29 Uhr MEZ
Nur gültig bis	Montag, 1. Juli 2019 1:59 Uhr MESZ
Öffentlicher Schlüssel	
Algorithmus	RSA-Verschlüsselung (1 2 840 113549 1 1 1)
Parameter	Ohne
Öffentlicher Schlüssel	256 Byte : E9 9B C3 67 85 F9 0D AE ... ➤
Exponent	65537
Schlüssellänge	2048 Bit
Schlüsselverwendung	Überprüfen

Screenshot by Till Tantau

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail


Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften
► Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

43-25

Kaskaden von Unterschriften

Deutsche Telekom Root CA 2

 **Deutsche Telekom Root CA 2**
Root-Zertifizierungs-Instanz
Gültig bis: Mittwoch, 10. Juli 2019 1:59 Uhr MESZ
Dieses Zertifikat ist gültig.

► Vertrauen
▼ Details

Name des Inhabers	
Ländername	DE
Organisation	Deutsche Telekom AG
Organisationseinheit	T-TeleSec Trust Center
Allgemeiner Name	Deutsche Telekom Root CA 2
Name des Ausstellers	
Ländername	DE
Organisation	Deutsche Telekom AG
Organisationseinheit	T-TeleSec Trust Center
Allgemeiner Name	Deutsche Telekom Root CA 2
Seriennummer	38
Version	3
Signaturalgorithmus	SHA-1 mit RSA-Verschlüsselung (1 2 840 113549 1 1 5)
Parameter	Ohne
Erst gültig ab	Freitag, 9. Juli 1999 14:11 Uhr MESZ
Nur gültig bis	Mittwoch, 10. Juli 2019 1:59 Uhr MESZ
Öffentlicher Schlüssel	
Algorithmus	RSA-Verschlüsselung (1 2 840 113549 1 1 1)
Parameter	Ohne
Öffentlicher Schlüssel	256 Byte : AB 0B A3 35 E0 8B 29 14 ... ➤
Exponent	65537
Schlüssellänge	2048 Bit
Schlüsselverwendung	Überprüfen

Screenshot by Till Tantau

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele
Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften
► Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen

43-25

Kaskaden von Unterschriften

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

- Ziele
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

- Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen

Schlüsselbundverwaltung

Klicken Sie hier, um den Schutz des Schlüsselbunds „System-Roots“ aufzuheben

Schlüsselbunde

- Anmeldung
- System
- System-Roots

Deutsche Telekom Root CA 2

Root-Zertifizierungs-Instanz
Gültig bis: Mittwoch, 10. Juli 2019 1:59 Uhr MESZ
✓ Dieses Zertifikat ist gültig.

Name	Art	Verfällt
Deutsche Telekom Root CA 2	Zertifikat	10.07.2019 00:00:00
Entrust.net Client Certification Authority	Zertifikat	12.10.2019 00:00:00
Entrust.net Certification Authority (2048)	Zertifikat	24.12.2019 00:00:00
Entrust.net Secure Server Certification	Zertifikat	04.02.2020 00:00:00
Entrust.net Client Certification Authority	Zertifikat	07.02.2020 00:00:00
Staat der Nederlanden Root CA - G2	Zertifikat	25.03.2020 00:00:00
DoD CLASS 3 Root CA	Zertifikat	14.05.2020 00:00:00
AddTrust Class 1 CA Root	Zertifikat	30.05.2020 00:00:00
AddTrust External CA Root	Zertifikat	30.05.2020 00:00:00
AddTrust Public CA Root	Zertifikat	30.05.2020 00:00:00
AddTrust Qualified CA Root	Zertifikat	30.05.2020 00:00:00
Equifax Secure eBusiness CA-1	Zertifikat	21.06.2020 00:00:00
Equifax Secure Global eBusiness CA-1	Zertifikat	21.06.2020 00:00:00

Kategorie

- Alle Objekte
- Kennwörter
- Zertifikate**
- Meine Zertifikate
- Schlüssel
- Sichere Notizen

163 Objekte

Screenshot by Till Tantau

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften
Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen ◀

- ▶ Wenn Sie mit einem Online-Shop oder Ihrer Bank kommunizieren, haben Sie *dieselben Problem wie bei E-Mail*:
 - ▶ Niemand soll die Kommunikation abhören können.
 - ▶ Sie müssen sicher sein können, dass Ihre Bank auch wirklich Ihre Bank ist.
- ▶ Diese Probleme werden auch genauso gelöst:
 - ▶ Die Bank oder der Online-Shop hat ein Schlüsselpaar, dass nun aber *keine Person* identifiziert sondern *eine Webseite*.
 - ▶ Das Schlüsselpaar ist über eine Kette von CAs unterschrieben.
- ▶ Die Protokolle *https* und *ssh* bauen auf diese Art sichere Kanäle auf.

Sicheres Surfen funktioniert wie sichere E-Mail.

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

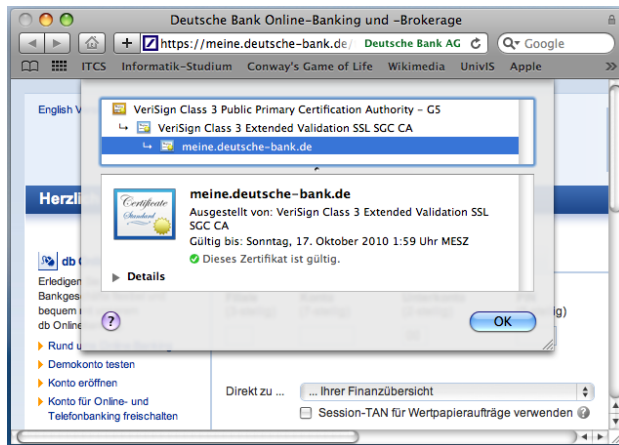
43.2 Verschlüsselung

- Ziele
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung

43.3 Sichere E-Mail

- Vertraulichkeit: Digitale Briefumschläge
- Authentizität: Digitale Unterschriften
- Echtheits-Zertifikate: Digitale Notare

43.4 Sicheres Surfen ◀



Screenshot by Till Tantau

Sicheres Surfen funktioniert wie sichere E-Mail.

Kapitel 43 Kommunikations- Sicherheit

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

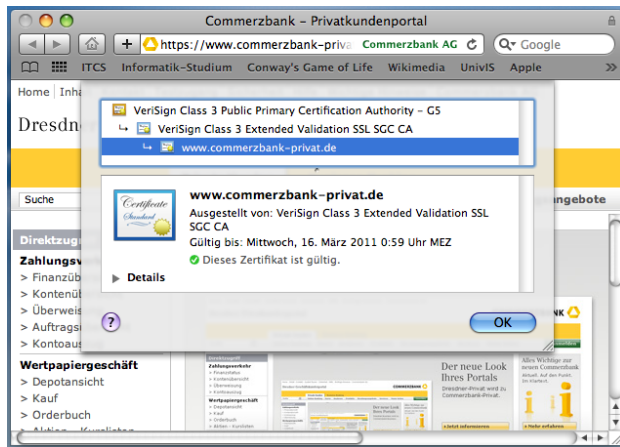
Ziele

Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften
Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen



Screenshot by Till Tantau

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften
Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen ◀

Symmetrische Verschlüsselung

Eine Nachricht m wird mit einem Schlüssel k zu einem Chiffre $c = e(m, k)$ verarbeitet. Mit *demselben* Schlüssel k lässt sich dann $m = d(c, k)$ berechnen. Das Standardverfahren heißt AES.

Asymmetrische Verschlüsselung

Eine Nachricht m wird mit einem *öffentlichen Schlüssel* k_e zu einem Chiffre $c = e(m, k_e)$ verarbeitet. Mit einem *ganz anderen* Schlüssel k_d lässt sich dann $m = d(c, k_d)$ zurückgewinnen. Das Standardverfahren heißt RSA.

43.1 Ziele von IT-Sicherheit

43.2 Verschlüsselung

Ziele

Symmetrische
Verschlüsselung
Asymmetrische
Verschlüsselung

43.3 Sichere E-Mail

Vertraulichkeit: Digitale
Briefumschläge
Authentizität: Digitale
Unterschriften
Echtheits-Zertifikate:
Digitale Notare

43.4 Sicheres Surfen ◀

Vertraulichkeit

Die *Vertraulichkeit* von E-Mails und der Kommunikation mit Webservern (https) wird sichergestellt, indem mit dem *öffentlichen Schlüssel des Empfängers* verschlüsselt wird.

Authentizität

Die *Authentizität* einer Nachricht wird sichergestellt, indem mit dem *privaten Schlüssel des Absenders* verschlüsselt wird. Dies nennt man *digitale Unterschrift*.

Zertifikate

Ein *digitales Zertifikat* ist ein von einer *Certificate Authority* unterschriebener Text, der bezeugt, dass ein öffentlicher Schlüssel zu einer bestimmten Person gehört.