Informationstechniken

HOCHSCHULE DER MEDIEN

KRYPTOGRAPHIETECHNIKEN FÜR NETZWERKSICHERHEIT UND E-COMMERCE

Prof. Dr. Wolf-Fritz Riekert
Hochschule der Medien (HdM) Stuttgart
Stuttgart Media University

Unter Mitwirkung von
Abraham Taherivand
Volz Innovation GmbH, Karlsruhe

KRYPTOGRAPHIETECHNIKEN: EIN AKTUELLES BEISPIEL

SPIEGEL ONLINE

01. April 2008,
16:01 Uhr

GEKNACKTER CODE

Deutsche Forscher öffnen Autos und Garagentore

Von Christian Stöcker

Auto- und Garagenbesitzer sollten sich vorsehen: Der Funk-Code für Abertausende von Toren und Wagentüren ist geknackt. Mit sehr einfachen Mitteln ließe sich so Zugang zu Autos und Wohnhäusern gewinnen. Das nötige Zubehör gibt es im Baumarkt.

Quelle: http://www.spiegel.de/netzwelt/tech/0,1518,544670,00.html

KRYPTOGRAPHIETECHNIKEN: EIN AKTUELLES BEISPIEL

Spionage: Alle großen Geheimdienste aktiv gegen deutsche Firmen

Größte Gefahr geht von China, Russland und dem nahen Osten aus

28. August 2007

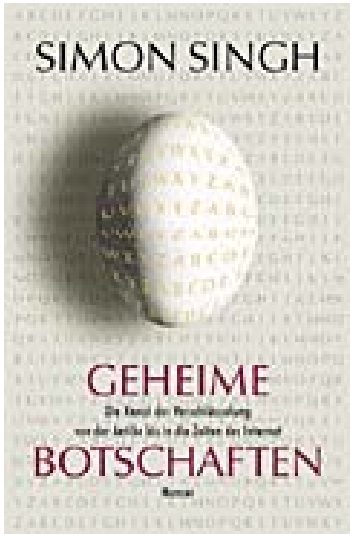
Die aktuellen Berichte über chinesische Spionage-Trojaner in deutschen Ministerien verdeutlichen, in welcher Gefahr insbesondere deutsche Mittelständler schweben. Der Sensibilisierung der Mitarbeiter kommt beim Kampf gegen Wirtschaftsspione eine tragende Rolle zu.

„Diese Angriffstechniken werden auch gegen Unternehmen eingesetzt und diese Spionage kostet Arbeitsplätze, darauf kann nicht deutlich genug hingewiesen werden", warnt Professor Hartmut Pohl, IT-Sicherheitsexperte an der Fachhochschule Bonn-Rhein-Sieg. „Damit sich Unternehmen gegen diese Angriffe schützen können, müssen die gefundenen Angriffsprogramme unverzüglich veröffentlicht werden."

Auch Thomas Pütz, der sich im Rahmen seiner Diplomarbeit an der Universität Siegen intensiv mit dem Thema Wirtschaftspionage beschäftigt hat, berichtet gegenüber der Computer Zeitung: „Die gezielte Nutzung von speziellen Spionage-Trojanern gegen deutsche Firmen wird vom Bundesamt für Verfassungsschutz in Köln bestätigt. Die Quelle solcher Angriffe wird in China vermutet."

Quelle: http://microsite.computerzeitung.de/article.html?art=/articles/2007036/31204916_ha_CZ.html&page=2&ms=/awareness-ll/index.html&pos=6&tpid=ee54f3c7-0de1-40f5-bb23-2cfdf022aee5&pid=17313f77-31da-4f96-8955-7bcd430e79bb

LITERATUREMPFEHLUNG



Simon Singh

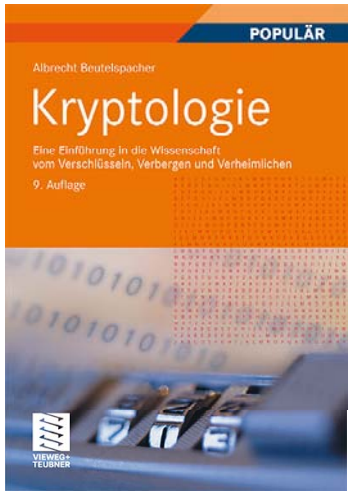
Geheime Botschaften

Carl Hanser; 5. Aufl. (2000)

Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet Geheime Botschaften hat es immer gegeben: Von Cäsar über Maria Stuart bis hin zur ENIGMA-Maschine und zum Computerzeitalter. Was früher nur die Mächtigen interessierte, ist heute, wo immer häufiger persönliche Daten im Internet zirkulieren, für jeden relevant. Alles über Geheimsprachen, Codes und deren Entschlüsselung in einem spannenden Wissenschaftskrimi von Simon Singh.

LITERATUREMPFEHLUNG

HOCHSCHULE DER MEDIEN



Albrecht Beutelspacher

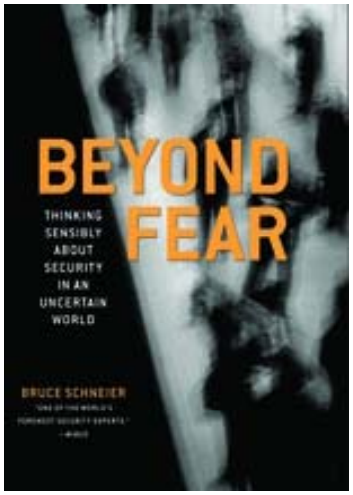
Kryptologie

Vieweg+Teubner; 9. Aufl. (2009)

Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen. Ohne alle Geheimnis-krämerei, aber nicht ohne hinterlistigen Schalk, dargestellt zum Nutzen und Ergötzen des allgemeinen Publikums. Das Buch bietet eine reich illustrierte, leicht verdauliche und amüsante Einführung in die Kryptologie.

LITERATUREMPFEHLUNG

HOCHSCHULE DER MEDIEN



Bruce Schneier

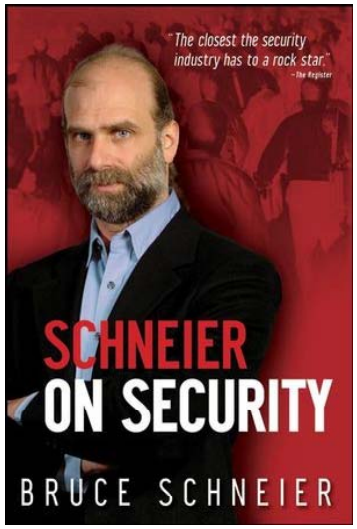
Beyond Fear
Thinking Sensibly About Security in an Uncertain World

Springer; Corr. 2nd printing (2006)

Many of us, especially since 9/11, have become personally concerned about issues of security, and this is no surprise. In Beyond Fear, Bruce Schneier invites us to take a critical look at not just the threats to our security, but the ways in which we're encouraged to think about security by law enforcement agencies, businesses of all shapes and sizes, and our national governments and militaries.

LITERATUREMPFEHLUNG

HOCHSCHULE DER MEDIEN



Bruce Schneier

Schneier on Security

Wiley & Sons (2008)

Presenting invaluable advice from the world's most famous computer security expert, this intensely readable collection features some of the most insightful and informative coverage of the strengths and weaknesses of computer security and the price people pay – figuratively and literally – when security fails. Discussing the issues surrounding things such as airplanes, passports, voting machines, ID cards, cameras, passwords, Internet banking, sporting events, computers, and castles, this book is a must-read for anyone who values security at any level -- business, technical, or personal.

LITERATUREMPFEHLUNG

HOCHSCHULE DER MEDIEN

Kevin D. Mitnick, William Simon

Die Kunst der Täuschung: Risikofaktor Mensch

Mitp-Verlag (2006)

Kevin Mitnick, einst der meistgesuchte Verbrecher der USA, saß fünf Jahre im Gefängnis, weil er in zahlreiche Netzwerke großer Firmen eingebrochen war. Dabei bediente er sich häufig nicht nur seiner umfassenden technischen Hacker-Kenntnisse, sondern überlistete praktisch jedes Sicherheitssystem, indem er sich Passwörter erschlich, in Mülltonnen nach sicherheitsrelevanten Informationen suchte und falsche Identitäten vorgaukelte.

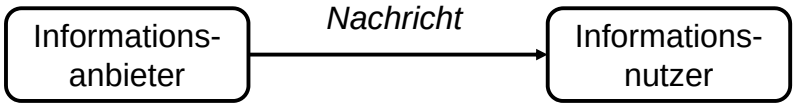
GEFAHREN DURCH MISSBRAUCH VON COMPUTERNETZEN

HOCHSCHULE DER MEDIEN

- Vandalismus
  - ⇨ Zerstörung von Informationen
  - ⇨ öffentliche Blamagen
- Wirtschaftskriminalität
  - ⇨ Betrug
  - ⇨ Diebstahl
  - ⇨ Erschleichung von Dienstleistungen
- Entwendung vertraulicher Informationen
  - ⇨ Industriespionage
  - ⇨ Verletzung der Privatsphäre

ANSATZPUNKTE FÜR ANGRIFFE AUF DIE SICHERHEIT IM INTERNET

HOCHSCHULE DER MEDIEN



- Einrichtungen des Informationsanbieters (Server)
  - ⇨ Möglicher Schutz: z.B. Firewall
- Einrichtungen des Informationsnutzers (Client)
  - ⇨ Möglicher Schutz: z.B. Antivirenprogramme
- Übertragene Informationen (Nachrichten)
  - ⇨ Möglicher Schutz: **Kryptographie**
  - ⇨ **Thema dieser Lehreinheit**

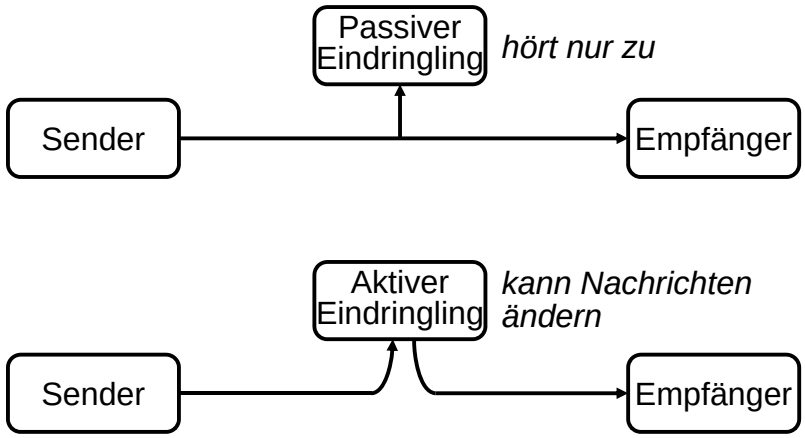
BEGRIFFE

HOCHSCHULE DER MEDIEN

Chiffre	Verschlüsselungsverfahren für Nachrichten (einschließlich zugehörigem Entschlüsselungsverfahren)
Kryptographie	Entwerfen von Chiffren
Kryptoanalyse	Aufbrechen („Knacken“) von Chiffren
Kryptologie	Wissenschaft der Verschlüsselung, umfasst Kryptographie und Kryptoanalyse
Klartext	(engl. plain text) zu verschlüsselnde Nachricht
Chiffretext	(engl. cypher text) verschlüsselte Nachricht
Verschlüsselung	(engl. encryption) Umsetzung von Klartext in Chiffretext
Entschlüsselung	(engl. decryption) umgekehrter Vorgang

EINDRINGEN IN NETZE

HOCHSCHULE DER MEDIEN



ÜBERTRAGUNGSSICHERHEIT DURCH KRYPTOGRAPHIE

HOCHSCHULE DER MEDIEN

Schutzgut	**Maßnahme**
Vertraulichkeit	digitale Verschlüsselung
Authentizität	digitale Zertifikate
Verbindlichkeit	digitale Signierung
Integrität	Message Digests (Prüfcodes)

DIE „CAESAR“-CHIFFRE – EIN EINFACHES BEISPIEL:

HOCHSCHULE DER MEDIEN

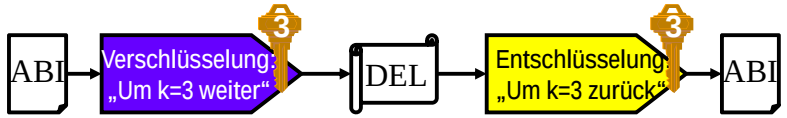
V **Verschlüsselungsverfahren:**
„Gehe in alphabetischer Reihenfolge um k Buchstabenpositionen weiter!“

3 **Schlüssel** k = 3

E **Entschlüsselungsverfahren:**
„Gehe in alphabetischer Reihenfolge um k Buchstabenpositionen zurück!“

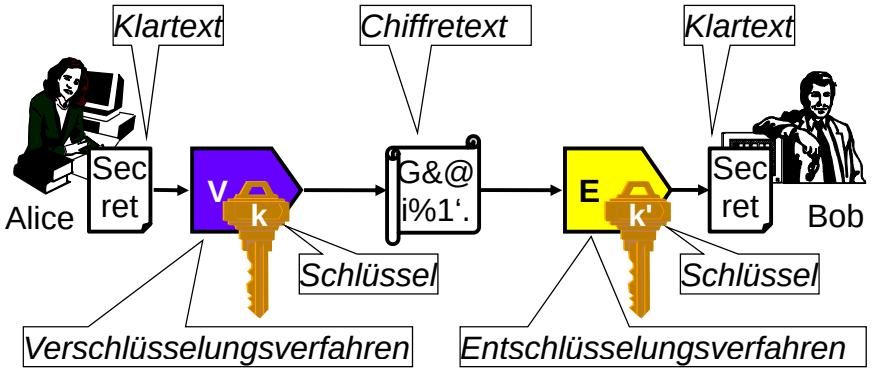
A → D
B → E
C → F
...
W → Z
X → A
Y → B
Z → C

Für Verschlüsselung und Entschlüsselung wird hier derselbe Schlüssel k verwendet.
⇒ **Symmetrisches Verschlüsselungsverfahren.**



VERSCHLÜSSELUNG (1)

HOCHSCHULE DER MEDIEN



Senderin Übertragung Empfänger

VERSCHLÜSSELUNG (2)

HOCHSCHULE DER MEDIEN

Eine **Verschlüsselung V_k** ist festgelegt durch zwei Vorgaben:

- ein allgemeines **Verschlüsselungsverfahren V** (auch Verschlüsselungsalgorithmus genannt, realisiert durch ein Programm),
- einen **Schlüssel** (Key) **k** (ein Zahlencode oder eine Zeichenkette), der das Verfahren einstellt (parametrisiert).

V k

Für die **Entschlüsselung $E_{k'}$** gilt Entsprechendes, diese ist festgelegt durch:

- ein allgemeines **Entschlüsselungsverfahren E,**
- einen **Schlüssel k'**, der das Verfahren einstellt (parametrisiert).

E k'

WORIN BESTEHT DAS GEHEIMNIS?

HOCHSCHULE DER MEDIEN

Was muss geheim gehalten werden, damit kein Unberechtigter an die verschlüsselten Informationen kommt?

- Der Verschlüsselungsalgorithmus?
  - ⇨ „Security by obscurity“ (Niemand weiß, wie die Verschlüsselung funktioniert
  - ⇨ Nicht empfehlenswert: Der Algorithmus kann Schwächen haben und niemand kann diese aufdecken.
- Der Schlüssel?
  - ⇨ Ja, das entspricht dem heutigen Stand der Technik
  - ⇨ Der Algorithmus soll so leistungsfähig sein, dass er offengelegt werden kann

KRYPTOANALYSE: AUFBRECHEN VON CHIFFREN

HOCHSCHULE DER MEDIEN

Drei Varianten der Kryptoanalyse:

- Nur Chiffretext
- Ein bekannter Klartext + zugehöriger Chiffretext
- Gewählter Klartext + Chiffretext

Fragen:

- Welche Varianten der Kryptoanalyse sind erwartungsgemäß vergleichsmäßig schwierig, welche vergleichsmäßig einfach?
- Welchen Varianten der Kryptoanalyse soll eine Chriffre mindestens widerstehen?

SYMMETRISCHE U. ASYMMETRISCHE VERSCHLÜSSELUNG

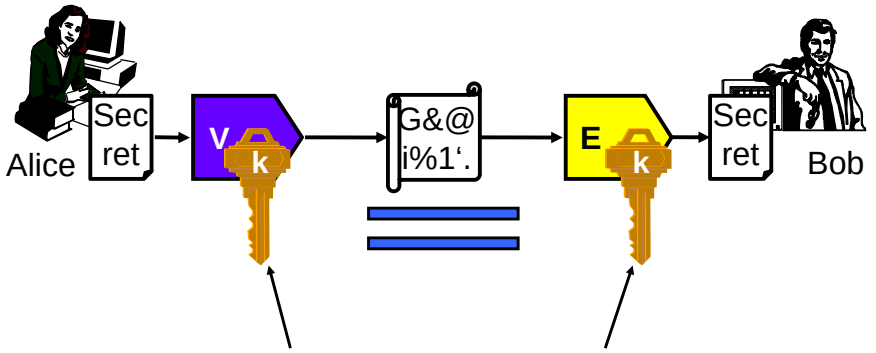
HOCHSCHULE DER MEDIEN

- **Symmetrische Verschlüsselung:**
  Für Entschlüsselung und Verschlüsselung wird derselbe Schlüssel k verwendet.
  - ⇨ Problem: Für jedes Paar von Kommunikations-partnern wird ein eigener Schlüssel benötigt.

- **Asymmetrische Verschlüsselung:**
  Für Entschlüsselung und Verschlüsselung werden unterschiedliche Schlüssel k und k‘ verwendet.
  - ⇨ Es gibt asymmetrische Verschlüsselungsmethoden, bei denen der Entschlüsselungsschlüssel k‘ praktisch nicht aus dem Verschlüsselungsschlüssel k abgeleitet werden kann.
  - ⇨ Mögliche Verwendung: sogenannte öffentliche Verschlüsselungsverfahren.

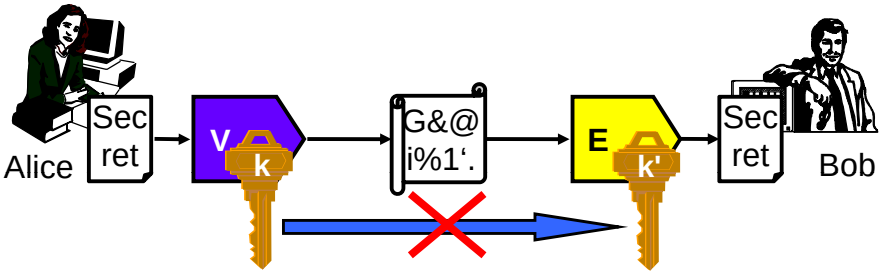
SYMMETRISCHE VERSCHLÜSSELUNG

HOCHSCHULE DER MEDIEN



Beide Schlüssel sind identisch:
Symmetrische Verschlüsselung

ASYMMETRISCHE VERSCHLÜSSELUNG



Der Entschlüsselungsschlüssel **k'**
kann mit vertretbarem Rechenaufwand nicht aus dem Verschlüsselungsschlüssel **k** abgeleitet werden:
Asymmetrische Verschlüsselung

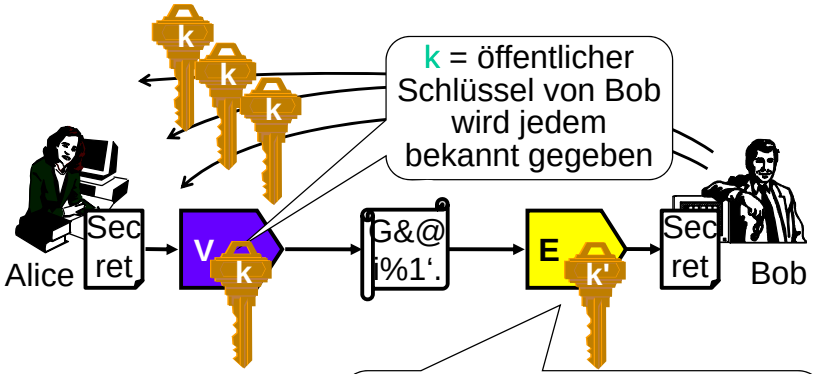
ÖFFENTL. VERSCHLÜSSELUNGS-VERFAHREN (1)

Asymmetrische Verschlüsselungsverfahren ermöglichen sogenannte öffentliche Verschlüsselungsverfahren:

- die **Verschlüsselung** erfolgt mit einem öffentlich bekannten Schlüssel k (dem **öffentlichen Schlüssel**).

- die **Entschlüsselung** mit einem nur dem Besitzer bekannten **privaten Schlüssel** k'.
- Es ist in der Praxis **unmöglich, k' aus k abzuleiten**. Ein solcher Versuch würde bei guten asymmetrischen Verschlüsselungsverfahren viele Jahre bis zum Erfolg benötigen, selbst wenn ein Supercomputer benutzt wird.

ÖFFENTL. VERSCHLÜSSELUNGS-VERFAHREN (2)



ÜBERTRAGUNGSSICHERHEIT DURCH KRYPTOGRAPHIE (W)

Schutzgut	**Maßnahme**
Vertraulichkeit	digitale Verschlüsselung
Authentizität	digitale Zertifikate
Verbindlichkeit	digitale Signierung
Integrität	Message Digests (Prüfcodes)

KOMBINATION ASYMMETR. UND SYMMETR. VERSCHLÜSSELUNG

HOCHSCHULE DER MEDIEN

- Um vertrauliche Nachrichten an Bob senden zu können, genügt ein öffentlicher Schlüssel für alle Absender.
- Nachteil: Asymmetrische Verschlüsselungsverfahren sind sehr aufwendig (erfordern viel Rechenleistung bzw. -zeit).
- Abhilfe: **Kombination mit symmetrischem Verschlüsselungsverfahren**. Alice erzeugt als erstes einen Schlüssel **s** für ein symmetrisches Verfahren, verschlüsselt diesen mit Bobs öffentlichen Schlüssel **k,** und schickt ihn in dieser Form auf sichere Weise an Bob.
- Mit dem symmetrischen Schlüssel **s** können Bob und Alice vertrauliche Nachrichten in beide Richtungen austauschen! Mit dem öffentlichen Schlüssel **k** wäre das nur in Richtung Bob möglich gewesen!

GÄNGIGE ASYMMETRISCHE VERSCHLÜSSELUNGSVERFAHREN

HOCHSCHULE DER MEDIEN

RSA = Bedeutendste asymmetrische Chiffre, wird in den meisten Verfahren mit öffentlichen und privaten Schlüsseln verwendet.

RSA = Anfangsbuchstaben der Nachnamen von Ronald **R**ivest, Adi **S**hamir und Leonard **A**dleman. Dies sind die Erfinder des Verfahrens und jetzt Professoren am Massachussetts Institute of Technology (MIT).

http://people.csail.mit.edu/rivest/Rsapaper.pdf

RSA Data Security: Firma für Kryptographie-Technologie, vertreibt RSA und andere Verschlüsselungsverfahren.

Alternative asymmetrische Chiffren mit ähnlichen Eigenschaften, aber geringerer Bedeutung: **Diffie-Hellman Key Exchange**, **ElGamal**, **DSS** (Digital Signature Standard).

GÄNGIGE SYMMETRISCHE VERSCHLÜSSELUNGSVERFAHREN

HOCHSCHULE DER MEDIEN

DES (Data Encryption Standard): genormt durch ANSI, 56-Bit-Schlüssel, heute innerhalb weniger Stunden knackbar.

Triple-DES: Dreifache Anwendung von DES, ist doppelt so sicher wie DES (d.h. entspricht 112-Bit), gilt als sicher.

IDEA (International Data Encryption Algorithm): benutzt 128-Bit-Schlüssel, gilt als sehr sicher, in Schweiz entwickelt.

RC2 (verschlüsselt Datenblöcke) und **RC4** (verschlüsselt Datenströme) erlauben Schlüssel zwischen 1 und 2048 Bits. Entwickelt und patentiert von RSA Data Security.

Rinjdael, entwickelt von J. Daemen und V. Rijmen, 2000 vom US-amerikanischen Normungsinstitut NIST zum Advanced Encryption Standard (**AES**) erklärt. Sehr schneller Algorithmus. Schlüssellängen 128, 192 und 256 BitS.

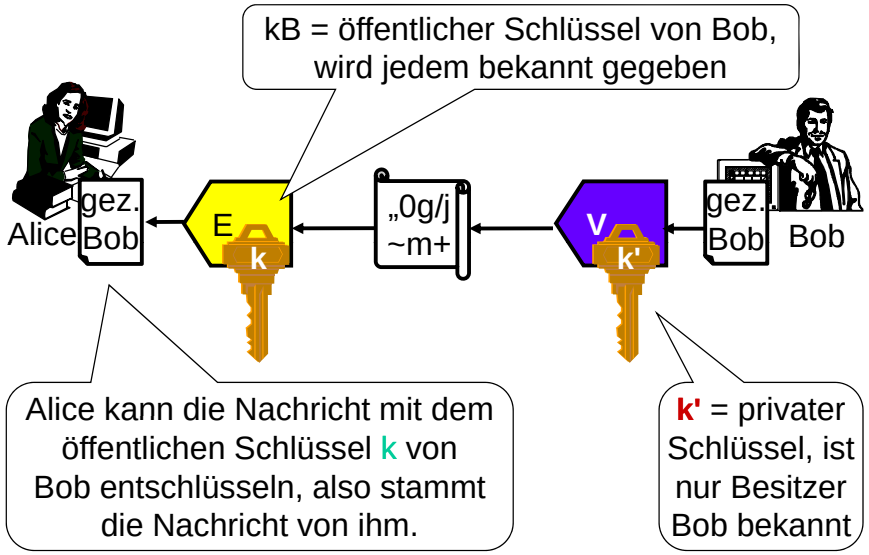
SIGNIERUNG: VERSCHLÜSSELUNG „IN UMGEKEHRTER RICHTUNG“

HOCHSCHULE DER MEDIEN

- Das asymmetrische Verschlüsselungsverfahren RSA (wie auch vergleichbare Verfahren) kann auch in umgekehrter Richtung betrieben werden.
- D.h., es wird eine Nachricht mit dem privaten Schlüssel verschlüsselt und mit dem öffentlichen Schlüssel entschlüsselt.
- Die Entschlüsselbarkeit mit dem öffentlichen Schlüssel ist der Beweis, dass die Nachricht vom betreffenden Absender stammt.
  - ⇨ Technische Grundlage für die **digitale Signierung** (**digitale Unterschrift**).

E-PERSONALAUSWEIS

DIGITALE SIGNIERUNG



VERSCHLÜSSELUNG UND SIGNIERUNG

- Verschlüsselung:
  - ⇨ Sender verwendet öffentlichen Schlüssel des Empfängers zur Verschlüsselung der Nachricht.
  - ⇨ Empfänger verwendet eigenen privaten Schlüssel zur Entschlüsselung der Nachricht.
- Digitale Unterschrift (Signierung):
  - ⇨ Die zu unterschreibende Nachricht wird mit dem privaten Schlüssel des Senders verschlüsselt. Das Ergebnis ist die unterschriebene Nachricht.
  - ⇨ Empfänger verwendet öffentlichen Schlüssel des Senders zur Entschlüsselung der Nachricht. Wenn diese Entschlüsselung gelingt, ist die „Unterschrift“ echt.

VERSCHLÜSSELUNG UND SIGNIERUNG: FOLGERUNGEN

Signierung und Verschlüsselung sind voneinander unabhängig möglich:

- Mit öffentlichen Schlüsseln verschlüsselte Nachrichten haben nicht notwendig eine Unterschrift. Sie können von jedermann stammen.
- Mit privaten Schlüsseln signierte Nachrichten sind nicht vertraulich. Sie können mit Hilfe des passenden öffentlichen Schlüssels von jedermann entschlüsselt werden.
- Verschlüsselung und Signierung können aber auch kombiniert werden. Hierzu verschlüsselt der Sender zunächst die Nachricht mit dem eigenen privaten Schlüssel (= Signierung) und dann mit dem öffentlichen Schlüssel des Empfängers (= Verschlüsselung).

INTEGRITÄT DURCH SIGNIERUNG VON MESSAGE DIGESTS

HOCHSCHULE DER MEDIEN

Signierung kann zur Gewährleistung der Integrität (Unverfälschtheit) von Nachrichten genutzt werden.

- Bob will Alice eine unverfälschbare Nachricht senden.
- Dazu bestimmt er aus der Nachricht einen Prüfcode, den sogenannten **Message Digest**.
- Bob signiert den Message Digest, d.h. er verschlüsselt ihn mit seinem privaten Schlüssel.
- Alice verifiziert Bobs Unterschrift, d.h. sie entschlüsselt den Message Digest mit Bobs öffentlichem Schlüssel.
- Alice berechnet den Message Digest aus der Nachricht und vergleicht ihn mit dem entschlüsselten Message Digest. Wenn beide gleich sind, ist die Integrität der Nachricht gesichert.

MESSAGE DIGESTS

HOCHSCHULE DER MEDIEN

Eigenschaften guter Verfahren zur Berechnung von Message Digests:

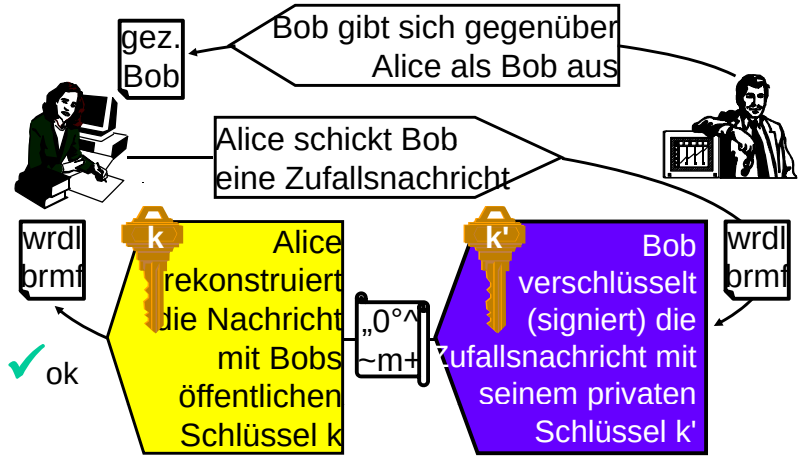
- Jedes Bit des Message Digests wird von jedem Bit der Nachricht beeinflusst.
- Wenn irgendein Bit der Nachricht verändert wird, kann sich jedes Bit des Message Digest mit 50% Wahrscheinlichkeit ändern.
- Wenn eine Nachricht und ihr Message Digest vorgelegt wird, sollte es mit heutigen technischen Mitteln unmöglich sein, eine zweite Nachricht mit demselben Message Digest zu erzeugen.

In der Praxis werden meist nur die Message Digests signiert und nicht die eigentlichen Nachrichten.

AUTHENTIFIZIERUNG

HOCHSCHULE DER MEDIEN

Mit Hilfe der Technik der Signierung können sich Kommunikationspartner ausweisen (authentifizieren):



KRYPTOGRAPHIE-INFRASTRUKTUR

HOCHSCHULE DER MEDIEN

Problem:

- Wie erfährt Alice den öffentlichen Schlüssel ihres Gesprächspartners, wenn sie zu ihm keine persönliche Verbindung hat?
- Wenn Sie den öffentlichen Schlüssel kennt, welche Gewissheit hat sie über die Identität des Gesprächspartners?

Abhilfe:

- Aufbau einer sog. „Kryptographie-Infrastruktur“.
- D.h.: Einrichtung von Zertifikatbehörden, sog. Certificate Authorities (CA) oder Trustcenters, die die Identität von Personen / Einrichtungen prüfen und deren öffentliche Schlüssel durch digitale Unterschrift beglaubigen.
- Diese Beglaubigung erfolgt mit sog. digitalen Zertifikaten.

DIGITALE ZERTIFIKATE

HOCHSCHULE DER MEDIEN

Zertifikate sind digitale Dokumente, die folgende Informationen enthalten:

- Angaben zur **Identität der Person/Institution** (Name, ggf. Adressangaben)
- **Öffentlicher Schlüssel** der Person/Institution
- **Ausgabedatum, Verfallsdatum**
- **Seriennummer**
- **Digitale Unterschrift des Trustcenters**
  - ⇨ kann mit öffentlichem Schlüssel des Trustcenters verifiziert werden.

Die derzeit gängige Norm für Zertifikate trägt die Bezeichnung **X.509 v3**

ARTEN VON ZERTIFIKATEN

HOCHSCHULE DER MEDIEN

Trustcenter unterscheiden **Zertifikate nach Einsatz**

- im Mailsystem: Verschlüsselung und Signierung (S/MIME)
- im Web-Server: Signierung von Webseiten, Initiierung einer sicheren Web-Verbindung (https)
- Signierung von Programmcode
- im Internet-Browser: Authentifizierung von Benutzern

Es werden Zertifikate in verschiedenen **Klassen** ausgegeben.

- Im einfachsten Fall: Legitimierung durch gültige Email-Adresse (nur für Privatpersonen, Zertifikat wird umgehend per Email zugeschickt).
- Für hohe Sicherheit: Legitimierung durch Personalausweis oder Reisepass und persönliches Erscheinen bei einer Behörde oder Agentur.

NORMEN UND PROTOKOLLE AUF BASIS VON X.509 V3

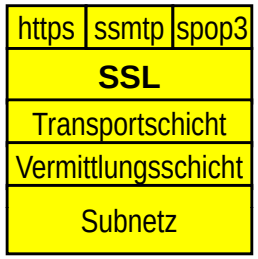
HOCHSCHULE DER MEDIEN

S/MIME: Erweiterung des MIME-Protokolls für Emails, erlaubt Verschlüsselung und Signierung mit Hilfe von X.509v3-Zertifikaten

SSL v3 (Secure Socket Layer) oder **TLS** (Transport Layer Secure): Zwischenschicht zwischen Verarbeitungsschicht und Transportschicht, realisiert sichere Transportverbindung zur Verschlüsselung und Signierung basierend auf X.509v3-Zertifikaten

Auf SSL aufbauende Protokolle (Auswahl):

- **https** (SSL-protected HTTP)
- **ssmtp** (SSL-protected SMTP)
- **spop3** (SSL-protected POP3)



SICHERE ÜBERTRAGUNG MIT HILFE VON ZERTIFIKATEN NACH X.509 V3

HOCHSCHULE DER MEDIEN

Alle modernen **Internet-Browser** und **Mailsysteme** (Internet Explorer, Outlook, Netscape, Mozilla, Firefox, Thunderbird) sind für Zertifikate nach X.509 v3 vorbereitet:

- Sie verstehen die Protokolle SSL v3 / TLS und S/MIME.
- Sie haben die öffentlichen Schlüssel der wichtigsten Trustcenter vorinstalliert.
- Dadurch ist eine sichere Kommunikation mit Teilnehmern möglich, deren öffentliche Schlüssel von einem dieser Trustcenter mit Zertifikaten beglaubigt (d.h. signiert) sind.
  - ⇨ Man kann ihnen verschlüsselte Email schicken
  - ⇨ Man kann deren digitale Unterschrift verifizieren
  - ⇨ Man kann mit diesen Teilnehmern eine verschlüsselte Kommunikation über das Web führen

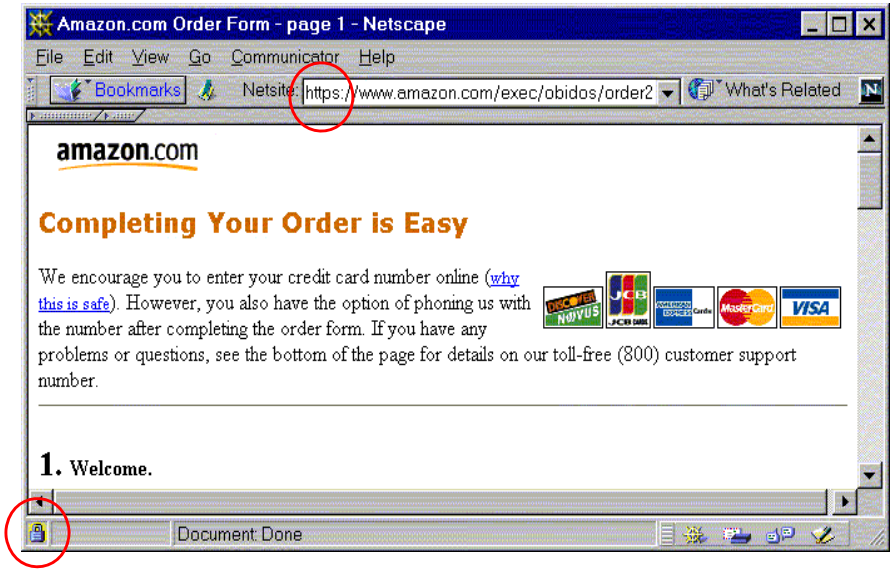
ANBIETER VON KRYPTOGRAPHIEVERFAHREN

HOCHSCHULE DER MEDIEN

- PGP (Pretty Good Privacy) von Network Associates (NA). Verfahren zur Verschlüsselung/Signierung von Email und Dateien. Entwickler Phil Zimmermann 1991. Hybrides Verfahren auf Basis von RSA und IDEA. Verfahren kommt ohne Trust Center aus. Frei für nichtkommerzielle Nutzer.
- Netscape / Mozilla / Firefox / Thunderbird: SSL/TLS-fähige Mailsysteme, Browser, Server und Trust-Center-Software
- Microsoft: SSL/TLS-fähige Mailsysteme Browser, Server und Trust-Center-Software
- Diverse Webserver-Anbieter (z.B. Apache): SSL-fähiger Webserver
- SSLeay: Freie Implementation von SSL (Eric Young)
- SSL Java: Implementationen von SSL in Java

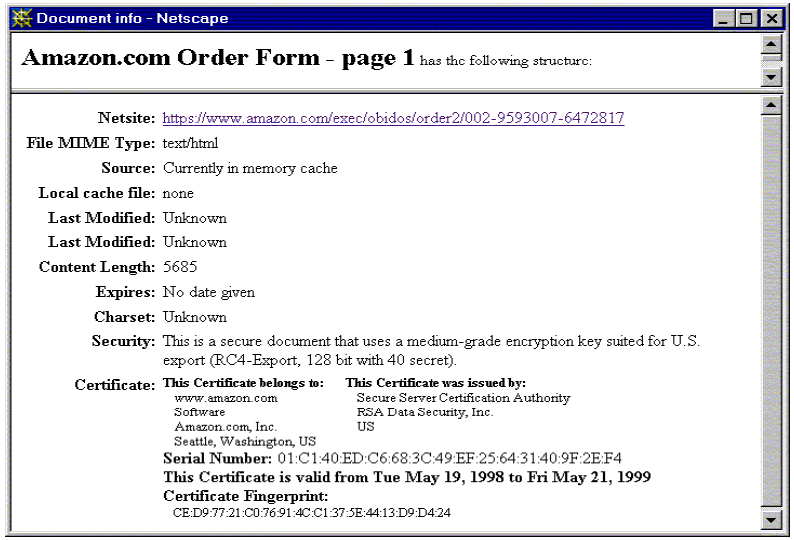
VERSCHLÜSSELTE KOMMUNIKATION MIT HTTPS UND SSL/TLS

HOCHSCHULE DER MEDIEN



DOKUMENTENINFORMATION ZU EINER SICHEREN WEBSEITE

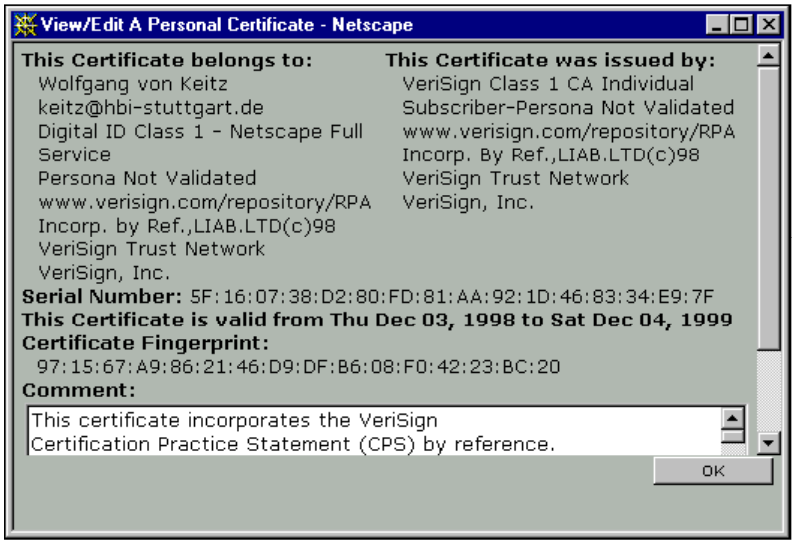
HOCHSCHULE DER MEDIEN



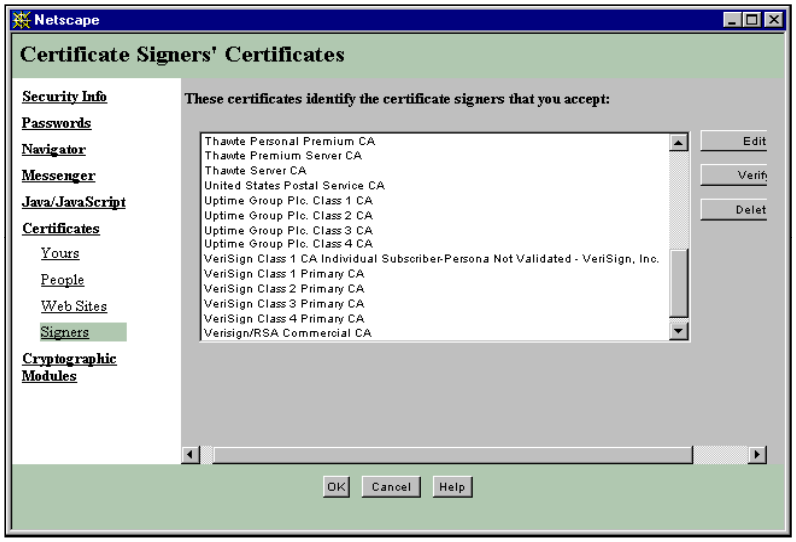
SIGNIERTE EMAILS MIT S/MIME

HOCHSCHULE DER MEDIEN

EIN DURCH EIN TRUST CENTER AUSGESTELLTES ZERTIFIKAT



VOM BROWSER AKZEPTIERTE TRUST CENTER



STEGANOGRAPHIE

Alternatives Verfahren zum Schutz von Nachrichten:

Steganographie = Verstecken von Nachrichten in einer anderen unverfänglichen Nachricht

Beispielsweise wird auf die Information in einem Bild oder einem Musikstück weitere Information gepackt, wobei das Bild bzw. das Musikstück unsichtbar bzw. unhörbar verändert wird.

Ggf. werden zusätzlich noch Kryptographietechniken angewandt.

Vorteil der Steganographie: Die Nachricht wird als solche von Uneingeweihten gar nicht erkannt.

INTERNET-BASIERTE ZAHLUNGSSYSTEME

- Meistverbreitetes digitales Zahlungssystem im Internet ist die **Kreditkarte**.
  - ⇨ Verschlüsselte Übertragung der Kartennummer mit SSL
  - ⇨ Klassische Methode der Transaktion mit Kreditkarte
  - ⇨ Dabei wird die Kartennummer dem Händler bekannt.
- **Neue Internet-basierte Zahlungssysteme** versuchen verschiedene Verbesserungen zu realisieren:
  - ⇨ Einfache Bezahlung ohne Eingabe von Kontonummern,
  - ⇨ Verringerte Transaktionskosten für Kleinstbeträge,
  - ⇨ Geheimhaltung der Bankverbindung des Kunden gegenüber Händler,
  - ⇨ oder gar völlige Anonymität des Kunden,
  - ⇨ Benutzbarkeit auch ohne Kreditkarte, z.B. durch Lastschrift vom Girokonto oder „digitale Münzen“.

ZAHLUNG PER KREDITKARTE

HOCHSCHULE DER MEDIEN

- Vor dem endgültigen Kaufabschluss übermittelt der Kunde per HTTPS seine Kreditkartennummer an den Händler.
- Ggf. gibt er weitere Zusatzinformationen an, z.B. Ziffern aus dem Unterschriftsfeld der Kreditkarte.
- Der Händler überprüft die Daten auf Plausibilität.
- Meist startet der Händler eine elektronische Rückfrage bei seiner Bank, die diese Rückfrage an die Bank des Kunden weiterleitet. Bei kleineren Beträgen und im Vergleich hohen Datenübertragungskosten kann dieser Schritt entfallen.
- Wenn alles ok ist, bestätigt der Händler den Kaufvorgang.
- Der Händler „bündelt“ mehrere solcher Verkaufsvorgänge und rechnet sie bei seiner Bank als „Stapel“ ab.

NEUE INTERNET-BASIERTE ZAHLUNGSSYSTEME

HOCHSCHULE DER MEDIEN

Es lassen sich zwei Arten neuer Internet-basierter Zahlungssysteme unterscheiden:

- **Anonyme Zahlungssysteme**: Weder der Betreiber des Zahlungssystems noch der Händler erfahren etwas über die Identität des Kunden bei einer Transaktion (ähnlich wie bei der Verwendung von Münzen oder Telefonkarten)
- **Private Zahlungssysteme**: Nur der Betreiber des Zahlungssystems braucht die Identität des Kunden zu erfahren, der Händler nur, wenn der Kunde das möchte (z.B. wegen Lieferadresse). Die Kaufdaten wiederum erfährt nur der Händler.

DIE WALLET (DIGITALE BRIEFTASCHE)

HOCHSCHULE DER MEDIEN

Für die am besten abgesicherten Internet-basierten Zahlungssysteme benötigt der Kunde eine **Wallet**, das ist eine Art „digitale Brieftasche“.

- Die Wallet ist eine Anwendung, die mit dem Internet-Browser kooperiert, wenn ein Kauf im Internet stattfindet.
- Die Wallet erhält man i.d.R. per Download vom Betreiber des Zahlungssystems.
- Die Wallet enthält alle für Transaktionen wichtigen Informationen, z.B. Zertifikate, private und öffentliche Schlüssel sowie ggf. auch Guthabenstände.
- Um sich vor dem Zahlungssystembetreiber sicher ausweisen zu können, muss der Kunde ein geeignetes **Zertifikat** erwerben und auf seiner Wallet installieren.

ANONYME ZAHLUNGSSYSTEME

HOCHSCHULE DER MEDIEN

Anonyme Zahlungssysteme funktionieren mit Hilfe digitaler Geldstücke (**Coins**).

- Der Kunde kann solche Coins von einer digitalen Münze (Mint) erwerben und in einer Wallet speichern. Der Wert wird dann von seinem Bank- oder Kreditkartenkonto abgebucht.
- Jedes Coin besteht aus einer eindeutigen Zeichenfolge und ist von der ausgebenden Mint signiert.
- Bezahlt wird durch Übersenden des Coins, d.h. der signierten Zeichenfolge an den Händler.
- Coins dürfen nur einmal ausgegeben werden. Der Händler tauscht die Coins sofort bei der Mint ein. Doppeltes Ausgeben eines Coins würde dabei als Betrug erkannt.
- Bekanntestes Beispiel: **DigiCash** (Dr. David Chaum, NL)
- Status: bisher erfolglos, DigiCash ging in Konkurs.

PRIVATE ZAHLUNGSSYSTEME

HOCHSCHULE DER MEDIEN

Typische Eigenschaften:

- Alle Teilnehmer (Kunde, Händler, Betreiber des Zahlungssystems) authentifizieren sich mit Zertifikaten.
- Alle Daten werden verschlüsselt übertragen.
- Die übertragenen Daten zerfallen in zwei Teile, die mit öffentlichen Schlüsseln von Händler bzw. Zahlungssystembetreiber verschlüsselt werden:
  - ⇨ Kaufdaten erhält nur der Händler.
  - ⇨ Die Identität und die Bankverbindung des Kunden erfährt nur der Zahlungssystembetreiber.
- Abbuchung von einem Konto des Kunden.
- Durch Authentifizierung des Kunden relativ sicher für Händler.

PRIVATE ZAHLUNGSSYSTEME: BEISPIELE

HOCHSCHULE DER MEDIEN

Beispiele privater Zahlungssysteme:

- **SET** (entwickelt von den Kreditkartenunternehmen Visa und Mastercard, weitere sind beteiligt):
  - ⇨ Abbuchung nur von Kreditkartenkonto.
- **CyberCash** (Partner einer Reihe großer Geldinstitute):
  - ⇨ Abbuchung von Kreditkartenkonto, von Girokonto oder von einem einfachen wiederaufladbaren Verrechnungskonto für Kleinstbeträge (**CyberCoin**).
- Beide Verfahren waren nicht erfolgreich
  - ⇨ SET hat sich nicht durchgesetzt, das Verfahren ist „schlafend“.
  - ⇨ CyberCash hatte keinen Erfolg, die Firma musste schließlich Konkurs anmelden

BEWERTUNG DER WALLET-BASIERTEN SYSTEME

HOCHSCHULE DER MEDIEN

Die Wallet-basierten Zahlungssysteme haben sich trotz der Vorteile für die Händler (relativ sichere Deckung der elekronischen Zahlung) allesamt **nicht auf dem Markt durchgesetzt**.

Gründe:

- Anlaufkosten bei den Händlern.
- Arbeitsaufwand beim Kunden: Installation von Software („Wallet“), Erwerb von Zertifikaten.
- Da Marktdurchdringung noch gering, Anreiz gering für neue Teilnehmer (Händler und Kunden) am Verfahren.

DERZEIT GEBRÄUCHLICHE ZAHLUNGSSYSTEME IM INTERNET

HOCHSCHULE DER MEDIEN

- Klassische Bezahlung per Kreditkarte via HTTPS (trotz der Nachteile: Umständliche Eingabe der Kreditkartendaten, weite Verbreitung von Kreditkartendaten, hohe Transaktionskosten, geringer Schutz für die Händler vor Betrug)
- „Ausfüllhilfen“ für die Verwendung von Kreditkarten:
  - ⇨ Microsoft Passport (Kreditkarteninfo wird auf Microsofts Passport Server gespeichert)
  - ⇨ Gator (Daten für HTML-Formulare werden lokal gespeichert)
- Neue webbasierte Zahlungssysteme ohne Wallet:
  - ⇨ PayPal (an Ebay Company)
  - ⇨ Click&Buy (Firstgate)
  - ⇨ WEB.Cent (web.de)
  - ⇨ ...

WEBBASIERTE ZAHLUNGSSYSTEME OHNE WALLET

HOCHSCHULE DER MEDIEN

Zahlungssysteme ohne Wallet sind relativ einfach nutzbar

- Der Kunde muss sich einmalig registrieren
- Ein Konto kann aufgeladen werden durch Bankeinzug oder Überweisung, manche Institute gewähren auch Kredit
- Beim Kauf identifiziert sich der Kunde per Passwort beim Institut, das Institut bestätigt dem Händler, das es für die Zahlung aufkommt.
- Gut geeignet für Micropayment immaterieller Güter.
- Beispiele:
  - ⇨ PayPal: insbeS.Ebay-Verkäufe, „Geldüberweisung“ per Email möglich, Paypal gewährt auch Kredit
  - ⇨ Firstgate: Click&Buy, gewährt auch Kredit
  - ⇨ WEB.Cent: Konto muss vor Kauf aufgeladen werden, Aufladung auch durch „Kaufrabatte“ möglich.

PAYPAL-VERIFIZIERUNG

HOCHSCHULE DER MEDIEN

Wie funktioniert der Verifizierungsprozess?

Durch die Verifizierung weisen Sie sich als geprüftes PayPal-Mitglied aus und können Ihr persönliches Kontolimit aufheben. Den Verifizierungsprozess leiten Sie durch Ihre Kreditkarte ein. Sie klicken einfach in Ihrem Profil auf „Verifizierung“. PayPal bittet Sie nun, Ihre Kreditkartendetails - sofern nocht nicht getan - einzugeben.

PayPal belastet nun Ihre Kreditkarte mit einer Gebühr von $1.95 USD. Der Belastungbetrag wird zusammen mit dem 4stelligen Bestätigungscode auf Ihrer nächsten monatlichen Kreditkartenabrechnung ausgewiesen.

Bei Online-Kreditkartenabrechnungen dauert es in der Regel je nach ausstellender Bank etwa 2-3 Arbeitstage bis der Bestätigungscode für die erweiterte Kontonutzung angezeigt wird.

Nach erfolgreich abgeschlossener Verifzierung schreibt Ihnen PayPal die $1.95 USD wieder gut, nachdem Sie die erste Zahlung über Ihre Kreditkarte geleistet haben. (Quelle Paypal)

Weitere Quellen

HOCHSCHULE DER MEDIEN

- http://www.thawte.com
- http://www.cacert.org
- http://www.versign.com
- http://www.nrca-ds.de/
- http://www.cryptool.de/
- http://www.philzimmermann.com/DE/background/index.html
- http://www.bsi.de/
- http://www.bsi.de/esig/index.htm