Modul 114

Kryptografie Teil 3

Digitale Signaturen

Digitale Signaturen

Repetition :

Symmetrische Verschlüsselung (Secret Key)

- ein geheimer Schlüssel steuert Chiffrieren und Dechiffrieren
- primäres Ziel : Vertraulichkeit
- Sogennant klassische Kryptographie.

Asymmetrische Verschlüsselung (Public/Privat Key)

- Chiffrieren und Dechiffrieren mit zwei verschiedenen Schlüsseln, die ein Schlüsselpaar bilden.
- Öffentlicher Schlüssel (public key, Chiffrierschlüssel) **ver**schlüsselt, wird öffentlich bekannt gemacht und beliebig verteilt.
- Privater Schlüssel (private key, Dechiffrierschlüssel) **ent**schlüsselt, liegt nur dem Empfänger vor und ist geheim.
- Nachrichten, die mit dem öffentlichen Schlüssel des Empfängers verschlüsselt wurden, können ausschliesslich mit dessen privatem Schlüssel entschlüsselt werden.

Repetition :

Asymmetrische Verschlüsselung (Public/Private Key)

- Sehr sicher (“hacken” scheitert an der Rechnerkapazität) nur 2 Schlüssel pro Teilnehmer
- Wer erzeugt Schlüsselpaare ? (Authentizität)

RSA

- Benannt nach Rivest, Shamir, Adleman
- Öffentlicher und privater Schlüssel hängen von einem Primzahlenpaar ab
- Sicherheit von RSA beruht auf speziellen mathematischen Funktionen, die nicht umkehrbar sind.
- Gebräuchliche Schlüssellängen :
  1024-bit (2004), 2048-bit, 3072-bit, 4096-bit
- Sowohl für Verschlüsselung als auch für digitale Signaturen

Die Problematik

- Wer bestellt in meinem E-Shop ?
- Wer schickt mir eine E-Mail ?
- Hat er wirklich das geschrieben was ich lese ?
- Woher kommt das Applet, das gerade auf meinen PC geladen wird ?
- Ist das Update wirklich das “richtige, unmanipulierte” Original ?
- Wohin wird meine Kreditkartennummer übermittelt ?
- Wer gibt einer Wahl gerade seine Stimme ab ?
- Stammt der Inhalt von “www.admin.ch” wirklich von unserer Regierung ?

Motivation

- Ausgehend von seinem Grundprinzip ist das Internet nicht sicher
- Mitlesen von Daten (Sniffing)
- Vortäuschen falscher Identitäten (Spoofing)
- Angriffe auf die Verfügbarkeit (Denial-of-Service)
- Übertragen von Programmen mit Schadfunktion (Viren, Würmer…)
- Menschliches Fehlverhalten (Preisgabe von geheimen Daten)

Sicherheit

- Sicherheit als Grundvoraussetzung für Nutzung des Internet in sensiblen Bereichen. (E-Commerce, E-Goverment, Gesundheitswesen)
- Geeignete technische und organisatorische Massnahmen als Voraussetzung für ein akzeptables Mass an Sicherheit.

- **Absolute Sicherheit ist nicht realisierbar !**
  Sinnvolles Verhältnis von Aufwand und Risiko.

Ziele Sicherheit

- **Authentisierung**
  Sicherstellung der Identität eines Kommunikationspartners
- **Vertraulichkeit**
  Zugänglichkeit der Nachrichteninhalte nur für einen bestimmten Empfängerkreis
- **Integrität**
  Schutz vor Verfälschung von Nachrichten bei der Übermittlung
- **Autorisierung**
  Prüfung der Zugriffsberechtigung auf Ressourcen
- **Verfügbarkeit**
  Schutz vor Verlust von Daten, Sicherstellung des laufenden Betriebs
- **Verbindlichkeit**
  Sicherer Nachweis der Absendung/des Empfangs von Nachrichten

Wesentlicher Ablauf

- Abbildung des Nachrichteninhaltes auf eine eindeutige Kenngrösse : Hash-Algorithmus
- Identifikation von Kommunikationspartnern durch Digitale Signaturen

Hash Algorithmus

- Bilden einen beliebig langen Nachrichtentext auf einen Wert vorgegebener (kurzer) Länge an (Hashwert, “Prüfsumme”)
- Aus Hashwert kann ursprüngliche Nachricht nicht errechnet werden (Irreversibilität)
- Konstruktion von Nachrichten mit gleichem Hashwert muss praktisch unmöglich sein
- zufällige Übereinstimmung von Hashwerten beliebiger Nachrichten unwahrscheinlich (Kollisionsresistenz, Integrität prüfbar)

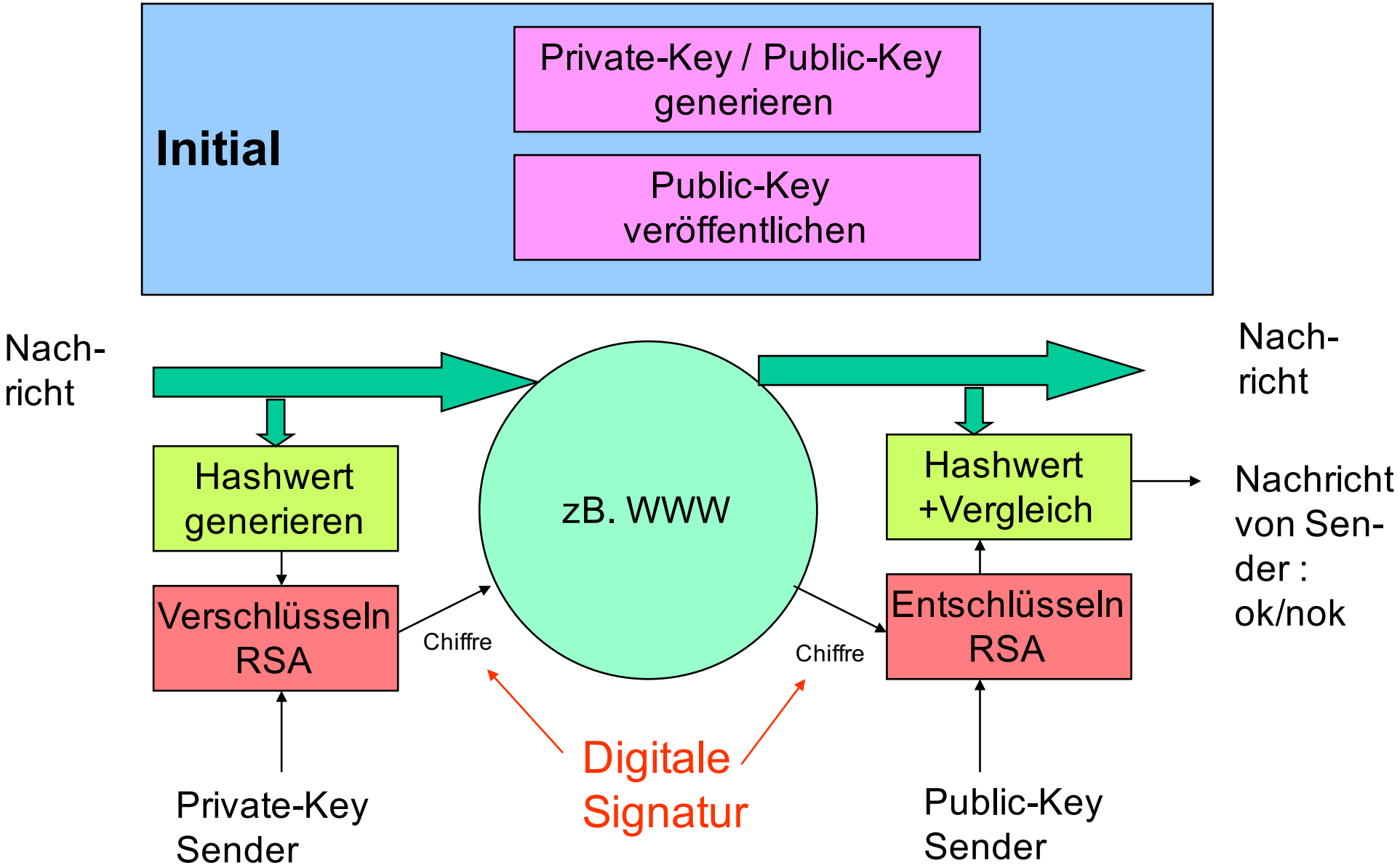
Digitale Signatur

- (Sichere) Identifizierung des Absenders eines Dokumentes
- Sicherheit vor nachträglichen Manupulationen des Dokumentes
- Elektronisch signierte Dokumente sind mit unterschriebenen Papierdokumenten gleich gesetzt
- Signaturen auch ohne Bezug zum Signaturgesetz möglich (eingeschränkte Sicherheit)

Digitale Signatur

- Ist ein Prüfwert einer Information
- Mit privatem Schlüssel verschlüsselt und zur Information hinzugefügt
- Der Empfänger kann mit Hilfe des öffentlichen Schlüssel des Senders prüfen, ob die Information wirklich vom Absender stammt und nicht verändert wurde.
- Die Digitale Signatur hat die Aufgabe einer Unterschrift und eines Sigels.

Ablauf : Digitales Signieren mit RSA :



Public Key Infrastruktur

- **OpenPGP (ein dezentraler Standard)**
  Anfangs 90‘ Jahre durch Phil Zimmermann entwickelt :
  Jeder Teilnehmer am Verschlüsselungssystem, der ein gültiges Schlüsselpaar besitzt, kann die Echtheit anderer Schlüssel durch seine Unterschrift bestätigen.

- **X.509 (zentral und hierarchisch organisiert)**
  der Besitzer hat seine Identität/Glaubwürdigkeit durch ein X-509 Zertifikat von einer **CA** (=**C**ertification **A**uthority) bescheinigen lassen
  Das heisst : Personenangaben werden mit dem Schlüsselpaar gekoppelt (Elektronischer Ausweis), ausgestellt von einer vertrauenswürdigen Instanz **TC** (=**T**rust **C**enter) oder CA

Aufgaben von TC’s bzw. CA's (X.509)

- Zertifikate ausstellen :
  Korrekte Identifikation des Teilnehmers,
  Zertifizieren von User, Server, Sub CA's
  Erstellung des Zertifikates durch digitale Signatur über Identifikationsdaten und öffentlichen Schlüssel eines Teilnehmers
- Bei Ausgabe eines Zertifikates an einen Teilnehmer ist dieser über Funktionalität und Gefahren von zertifizierten Signaturschlüsseln zu unterrichten
- Veröffentlichen der Public-Keys der User
- Publizieren eigenes Zertifikat
- Verwalten bzw. Archivierung angelaufener Zertifikate
- Zertifikate zurückziehen oder für ungültig erklären
- Festlegung der Gültigkeitsdauer von Zertifikaten
- Zeitstempeldienst Absicherung im Falle des Diebstahls des geheimen Schlüssels.Nachweis einer zeitpunktsbezogenen Willensbekundung. Nachweis und Sicherheit, dass die digitale Signatur nicht nach Ablauf der Gültigkeit des Zertifikates erstellt wurde.

Schwachstellen von RSA :

Aufgaben

Welche Zertifizierungs-Dienstleister nach X.509 sind in der Schweiz relevant?

Beurteilen Sie die Sicherheit von RSA (Verschlüsselung, digitale Signatur)

Was steckt hinter folgenden Stichworten:
Chosen Cyphertext
Man in the middle-Attack
Geburtstagsangriff
Erklären Sie diese!

Schwachstellen von RSA :

Chosen Cyphertext :	Unterschreiben sie nie irgendwelche binären Dateien unbekannten Inhalts mit ihrem privaten Schlüssel – es könnte sich um einen Chosen-Cipher-text-Angriff handeln. (=Man in the middle-Attack)
Geburtstagsangriff :	Unterschreiben Sie niemals ein Dokument, (auch wenn es für sie im Klartext abgefasst ist), das sie nicht selber verfasst haben. Es sei denn, sie nehmen vor der Unterzeichnung einige subtile Aenderungen vor. ZB. Vor der Unterzeichnung Einfügen von Leer-zeichen; Damit ändern sie wiederum den Hasch-wert der ihnen vorgelegten Daten und machen den Geburtstagsangriff zunichte.

Der Geburtstagsangriff

Eigentlich sollte Dokument und dazugehöriger Hashwert einmalig sein.
Dem ist leider nicht ganz so. Nach langem PC-unterstützten Suchen ist es möglich, zwei unterschiedliche Dokumente mit gleichem Hashwert zu finden!

1. Mallory erstellt zwei Versionen eines Dokumentes
   „Guter Text: Alice an Bob“ und „Böser Text: Alice an Mallory“
2. Mallory erstellt von beiden Dokumenten (Gut und Böse) je verschiedene Varianten. Der jeweilige Inhalt wird dabei geringfügig, dh. von Auge kaum erkennbar, abgeändert (zB. einfügen von Leerschläge etc.)
3. Mallory sucht „Gut“ und „Böse“ Varianten mit demselben Hash-wert (Die Wahrscheinlichkeit für ein Treffer ist relativ hoch!)
4. Mallory legt Alice die gefundene Variante von „Guter Text“ zur Unter-schrift vor.
5. Alice unterschreibt die „Guter Text: Alice an Bob“ für Bob
6. Mallory trennt nun die Signatur von „Guter Text“ ab und fügt sie „Böser Text: Alice an Mallory“ an.
7. „Böser Text: Alice an Mallory“ ist nun ebenfalls gültig !

Chosen Cyphertext

1. Mallory fängt verschlüsselte Nachricht an Bob ab und besorgt sich den Public-Key von Bob.
2. Mallory wählt Zufallszahl r (r<n und teilerfremd zu n)
3. Mallory : $x=r^e \bmod n$ (e=Public-Key von Bob)
4. Mallory : $y=x * c \bmod n$ (c=Nachricht)
5. Mallory überredet Bob dazu, die errechnete Nachricht y digital zu signieren.
6. Bob : $u=y^d \bmod n$ (d=Private Key von Bob)
7. Mallory : $r^{-1} * u \bmod n = r^{-1} * y^d \bmod n$
   $= r^{-1} * x^d * c^d \bmod n$
   $= r^{-1} * (r^e)^d * c^d \bmod n$
   $= r^{-1} * r * c^d \bmod n$
8. Die Exponenten e und d heben sich gegenseitig auf wie auch r und r^{-1}. Es bleibt übrig : $c^d \bmod n$ >>Die Klartextnachricht !!!