Kryptographie und Komplexität

Einheit 6.5

Anwendungsbeispiele

1. Online Auktionen
2. Elektronisches Geld
3. Online Voting
4. Car-2-car Kommunikation

Online Auktionen

- **Geheimes Bieten ohne Offenlegen der Finanzkraft**
  - Gebote werden in versiegeltem Umschlag (elektronisch) hinterlegt
  - Das höchste Gebot bekommt den Zuschlag
- **Erst-Preis Auktion** (holländische Auktion)
  - Auktionator beginnt mit Maximalpreis und geht schrittweise herunter bis ein Bieter das Angebot annimmt
  - Man zahlt das, was man maximal zu zahlen bereit ist
  - Bei versiegelten Geboten entspricht der erzielte Preis dem Preis des höchsten Gebots
  - Angebot sollte (knapp?) unter vermutetem tatsächlichen Wert sein
- **Zweit-Preis Auktion** (englische Auktion, eBay)
  - Auktionator beginnt mit Minimalpreis und geht schrittweise herauf bis kein Bieter mehr das Angebot annimmt
  - Man zahlt oft weniger, als man maximal zu zahlen bereit wäre
  - Bei versiegelten Geboten entspricht der erzielte Preis dem zweithöchsten Gebot (+ Festbetrag)
  - Angebot sollte dem vermuteten tatsächlichen Wert entsprechen

Iteriere Protokoll für anonymen Vergleich

- **Erst-Preis Auktion**
  - Bieter geben verschlüsselte Gebote beim Auktionator ab
  - Bieter vergleichen verschlüsselte Gebote untereinander anonym
  - Endgültiger Gewinner teilt sich dem Auktionator mit und gibt sein Angebot und seinen Schlüssel preis
  - Auktionator vergleicht anonym mit allen Bietern und bestätigt
  - Kaufpreis ist offengelegtes gebot des höchsten Bieters
- **Zweit-Preis Auktion** Strafmaßnahmen für Sabotage nötig
  - Bieter geben verschlüsselte Gebote beim Auktionator ab
  - Bieter vergleichen verschlüsselte Gebote untereinander anonym
  - Endgültiger Gewinner gibt teilt sich dem Auktionator mit
  - Verbleibende Bieter vergleichen erneut
  - Zweiter Gewinner legt Angebot und Schlüssel offen
  - Auktionator vergleicht anonym mit allen Bietern und bestätigt
  - Kaufpreis ist offengelegtes Gebot des zweithöchsten Bieters

Elektronisches Geld

- **Bargeldzahlung mit elektronischen Mitteln**
  - Mehr als electronic cash mit Bankkarte (Online Transaktion)
  - Bezahlvorgang muß ohne Angabe des Namens möglich sein
  - Man darf dem Zahler die Transaktion nicht nachweisen können
- **Anforderungen an elektronisches Geld**
  - Anonymität der Transaktion (Offline Transaktion)
  - Übertragbarkeit von Geld auf andere
  - Wechsel von größeren Beträgen in kleinere
  - Keine Mehrfachverwendung elektronischer Münzen
  - Effizente Durchführbarkeit auf Smartcards
- **Realisierung benötigt blinde Signaturen**
  - Alice verblendet Nachricht mit Blendungsfaktor
  - Bob (z.B. die Bank) signiert verblendete Nachricht
  - Alice entfernt Verblendung und erhält Signatur auf Originalnachricht

  Bob kann Alice nicht mit Originalnachricht in Verbindung bringen

Protokolle für Elektronisches Geld

- **Abheben einer Münze vom Konto**
  - Alice wählt Seriennummer und Blendungsfaktor
  - Nach blinder Unterzeichnung durch Bank hat Alice signierte Münze
  - Bank bucht Gegenwert vom Konto ab
- **Zahlungsvorgang**
  - Alice sendet Münze an Händler
  - Händler prüft Signatur und sendet Münze an die Bank
  - Bank bestimmt Seriennummer der Münze und prüft, ob Münze neu ist
  - Bank schreibt Händler das Geld gut
- **Ergänzungen der Grundprotokolle**
  - Im Betrugsfall muß Bank Identität des Betrügers feststellen können aber nicht, wenn Münze zum ersten Mal verwendet wurde
  - Bank muß betrügerischen Händler von betrügerischem Kunden trennen
  - Bank muß Betrugskooperation von Kunden und Händlern aufdecken

Online Voting

- **Wahlen über das Internet haben viele Vorteile**
  - Leichter als Briefwahl, wenn man nicht zum Wahlbüro gehen kann
  - Schnelle Auswertung des Ergebnisses
  - Vermutlich höhere Wahlbeteiligung

... aber auch Gefahren

  - Wahlmanipulation durch Organisatoren wird erleuichtert
    $\mapsto$ Wahlbetrugsanalyse mit statistischen Methoden
  - Wahlmanipulation durch Hacker wird möglich
    $\mapsto$ Sicherung von Kommunikation und Infrastruktur (Hard- & Software)
  - Stimmabgabe durch nicht-legitimierte Wähler, Identitätsdiebstahl
    $\mapsto$ Authentifizierungsprotokolle und (blinde) Signaturen
  - Stimmabgabe bleibt nicht geheim
    $\mapsto$ Zero-Knowledge Protokolle, Verschlüsselung, Hashfunktionen

Online Voting - Anforderungen und Probleme

- **Die Anonymität des Wählers muß garantiert werden**
  - Nur der Wähler kennt die von ihm ausgeübte Wahl (Geheime Wahl)
  - Er kann anderen nicht beweisen, wofür er gestimmt hat (Stimmenkauf)
- **Legitimierte Wähler können genau einmal wählen**
  - Keine doppelte Stimmabgabe, keine Wähler von außerhalb
  - Wähler dürfen ihre Stimme bis zu einem bestimmten Zeitpunkt ändern
- **Die Korrektheit des Ergebnisses ist gewährleistet**
  - Niemand kann die Ermittelung des korrekten Wahlergebnisses verhindern
  - Jeder Wähler kann prüfen, ob seine Stimme richtig gezählt wurde.
- **Fälschungen sind anfechtbar**
  - Wähler können Fehler bei der Zählung ihrer Stimme korrigieren
- **Die Wahl kann in einem Rechnernetz stattfinden**
  - Vertrauen besteht nur bei überzeugenden Sicherheitsmaßnahmen
  - Client-Rechner müssen gegen massive Angriffe von Außen gesichert sein
  - Die verwendete Systemsoftware darf keine Sicherheitslücke aufweisen

Mindestens so gut wie Wahlen mit Stimmzetteln

Protokolle für Online Voting

- **Stimmabgabe und Veröffentlichung des Wahlresultats**
  - Wähler registrieren sich
  - Wähler stimmen ab und unterzeichnen mit blinder Signatur
  - Administrator verifiziert Authorisierung, quittiert Stimme,
  - Wähler prüft Quittung und schickt Entschlüsselungscode
  - Zählsystem entschlüsselt Nachricht und zählt die anonyme Stimme
- **Protokoll zur Korrektur falscher Zuordnungen**
  - Wähler protestiert und schickt quittierte Stimme
  - Zählsystem prüft Quittung, tauscht alte Stimme aus und zählt neu
  - Wähler veröffentlicht Quittung, wenn er dem Ergebnis erneut mißtraut
- **Protokoll zur Änderung einer Stimme**
  - Wähler schickt Änderungswunsch mit (verschleierter) Quittung
  - Zählsystem legt quittierten Änderungswunsch ffen
  - Wähler schickt Stimmänderung, Zählsystem tauscht Stimme aus

Car-2-Car Kommunikation

Informationsaustausch zwischen Kraftfahrzeugen

- **Frühzeitige Warnung vor kritischen Situationen**
  - Sicherheit: Unfallvermeidung durch Gefahrenwarnung
    Aquaplaning, Glatteis, Pannenfahrzeuge, Falschfahrer, ...
  - Verkehrsfluß: Stauwarnung, spontane Baustellen,
    Ankündigung von Krankenwagen/Feuerwehr/Polizei
- **Technische Aspekte**
  - Lokale Datenerfassung: Position, Richtung, Geschwindigkeit, Lenkwinkel
  - Regionbezogene Daten: Straßenzustand, Verkehrsdichte
  - Schnelle Kommunikation zwischen entgegenkommenden Fahrzeugen
- **Wirtschaftliche Aspekte**
  - Ausrüstung von Fahrzeugen, intelligente Straßen, Satelliten, Mobilfunk

Anforderungen an Car-2-Car Kommunikation

- **Informationstechnische Aspekte**
  - Auswahl relevanter Daten zur Weitergabe an Dritte/Vierte etc.
  - Aktualitätskontrolle
  - Auswahl dringend erforderlicher Warnungen
- **Sicherheit vs. Datenschutz**
  - Signatur zur Vermeidung von Nachrichtenfälschung und Manipulation z.B. gezielte Fehlinformation zu Staus
  - Einhaltung der Privatsphäre verlangt Anonymisierung von Meldungen
  - Krimineller Mißbrauch muß Aufhebung der Privatsphäre ermöglichen
  - Verhinderung von Systemblockaden durch Denial-of-Service Attacken
- **Mögliche Probleme**
  - Was bedeutet es, wenn das System keine Warnungen meldet?
  - Wer schützte Fußgänger, Radfahrer und Fahrzeuge ohne Warnsystem ?
  - Wer verhindert dann automatische Strafzettel ?

Anwendungen von Kryptographie

- **Kryptographie ist die Grundlage für Sicherheit**
  – Verschlüsselungsverfahren zur Sicherung von Vertraulichkeit
  – Protokolle für Datenintegrität, Authentizität, Verbindlichkeit
  – Protokolle zur Sicherung und Aufhebung von Privatsphäre
- **Anwendungen haben viele weitere Aspekte**
  – Wirtschaftliche (ist die Technik bezahlbar?)
  – Soziologische (wird die Gesellschaft die Lösung akzeptieren?)
  – Juristische (wer haftet, wenn es schiefgeht?)
  – Politische (müssen Gesetze geändert / geschaffen werden?)
  – Psychologische (Kommt die Bevölkerung mit der Technik klar?)
- **Entwickler müssen Güter gegeneinander abwägen**
  – Eine ideale Lösung gibt es nicht - irgendjemand wird darunter leiden
  – Man muß einkalkulieren, daß manche Menschen völlig anders denken