Informatik II

4. Februar 2002

Prof. Bernt Schiele
ETH Zurich, Schweiz
http://www.inf.ethz.ch/~mavtinf/

schiele@inf.ethz.ch

Sicherheit in der Informationstechnologie

- Nur die Folien sind wichtig für die Prüfung
- Interessante Vorlesung:
  - Prof. Ueli Maurer, Informationssicherheit und Kryptographie, Departement Informatik
- Interessante Bücher:
  - Bruce Schneier: Applied Cryptography, John Wiley (allgemein verständlich)
  - Menezes, van Oorschot, Vanstone: Handbook of Applied Cryptography
  - Stinson: Cryptography - Theory and Practice

Sicherheit in der Informationstechnologie

- Warum ?
  - Internet gilt als unsicher
  - Datenschutz (Vorgaben per Gesetzgebung)
  - Digitalisierung der Wirtschaft (z.B. electronic commerce)

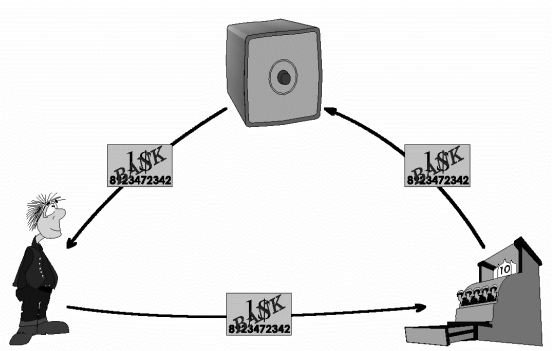
Anwendungen von Sicherheitstechnologie

- Sicherung von unsicheren (Daten)-Netzwerken
- sicherer elektronischer Handel
- online banking
- Benutzerauthentifikation (Bsp: Single Sign-on mittels Benutzerchipkarte, biometrische Verfahren)
- elektronischer Pass
- digitale Unterschrift
- digitale Zahlungssysteme (E-Cash)
- Urheberrechtsschutz
- anonyme und fälschungssicherer Abstimmungen und Wahlen
- ...

Einige Problemstellungen der Informationssicherheit

- sichere bilaterale Kommunikation (Vertraulichkeit, Authentizität)
- elementare Netzwerksicherheit
- sichere organisationsweite IT-Infrastruktur
- electronic commerce, Verbindlichkeit digitaler Verträge
- digitale Zahlungssysteme
- Datenschutz, Privacy
- Schutz von digitalem geistigem Eigentum
- ...

Digitales Zahlungssystem



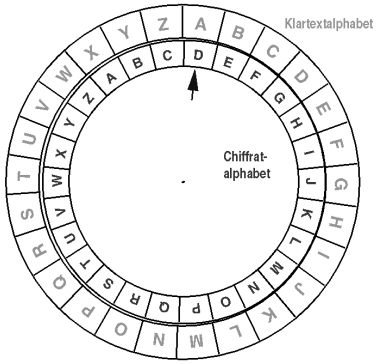
Anonymes digitales Geld (E-Cash) einige Probleme

- Fälschung
- mehrfaches Ausgeben
- Geldwaschproblematik
- perfekte Erpressung (risikolose Lösegeldübergabe)
- rechtliche Probleme (Haftung, Rechtsansprüche)
- finanztechnische Probleme (Bsp: Definition der Geldmengen)

Geschichte der Kryptographie

- Kryptographie in der Antike (z.B. Caesar) und im Mittelalter
- 1. Weltkrieg: Zimmermann Telegramm
- 2. Weltkrieg: Enigma, Alan Turing
- 1948 Shannon: Informationstheorie
- 1974 Data Encryption Standard (DES)
- 1976 Diffie und Hellman: Public-Key Kryptographie
- 1978 RSA: Erstes Signaturverfahren
- 1987 International Association for Cryptologic Research (IACS)
- seit ca. 1990: massive kommerzielle Nutzung

Verschlüsselung von Caesar



Elementare Sicherheitsanforderungen

- Vertraulichkeit bzw. Geheimhaltung
  - Information soll nur berechtigten Personen zugänglich sein
- Authentizität
  - d.h. verifizierbare Echtheit / Korrektheit der Information bzgl. Erzeuger, Empfänger, Inhalt, Zeit, etc.
  - Integrität (Unversehrtheit) ist spezieller Aspekt der Authentizität
- Verfügbarkeit
  - Information soll dem legitimierten Benutzer verfügbar sein

Bedrohungen

- Fehler und Störungen
  - fehlerhafte Übertragung
  - Stromausfall, Naturereignisse
  - Benutzerfehler
- intelligente Gegner
  - Hacker
  - unehrliche Mitarbeiter
  - kriminelle Organisationen
  - Geheimdienste

Liste möglicher Attacken (eines intelligenten Gegners)

- Stehlen von Datenträgern
- Eindringen in ein Benutzerkonto (Fälschung der Benutzerauthentifikation)
- Unerlaubtes Lesen, Löschen oder Verändern von Daten
- Abhören einer Datenleitung
- Einspeisen von Information in eine Datenleitung
- Abstreiten des Sendens/ Empfangs von Information
- „replayattack“ - nochmaliges Einspielen einer alten Meldung (Bsp: Geldüberweisung mehrfach verbuchen)
- Einschleusen von Viren
- ...

Sicherheitsziele

- Beweisbarkeit von Handlungen
  - Bsp: Empfang einer Meldung
- Anonymität von Benutzern
  - Bsp: Persönlichkeitsschutz bei digitalen Zahlungssystem
- Schutz von geistigem Eigentum
  - Bsp: Kopierschutz von software

Risikobehandlung

- Sicherheitspolice
  - welche Daten sind wie sensitiv
  - wer ist für was verantwortlich
- Risikoanalyse
  - mögliche Bedrohungen (Angreifer, Schwachstellen)
  - potentielle Schäden durch potentielle Attacken
  - Gewichtung nach geschätzte Eintrittswahrscheinlichkeit
  - Prioritäten für die kritischen Bereiche

Risikobehandlung

- Risikoreduktion
  - Risikovermeidung
  - Schutzmassnahmen
  - Konzept für Schadensbegrenzung (Katastrophenplan)
  - Schadenüberwälzung (Versicherungen)
- Akzeptieren des Restrisikos
  - kein System kann perfekt sicher sein
  - wichtiges Restrisiko: Mensch
  - bewusst Restrisiken identifizieren und akzeptieren

grundlegende Technologien

- Kryptographie
- Betriebssystemsicherheit (access control, firewalls)
- Prozessortechnologie (privilegierter Modus, Speicherzugriffsrechte)
- physisch sichere Module (Chipkarten)
- Biometrische Technologie
- Bautechnik (Sicherheitszonen, Brandschutz, Zutrittskontrollen, etc.)
- Schutz gegen elektromagnetische Einstrahlung und Abstrahlung
  - die Abstrahlung eines normalen Bildschirmes reicht aus, um den Bildschirminhalt auf einige 100m zu rekonstruieren

Krypto-...

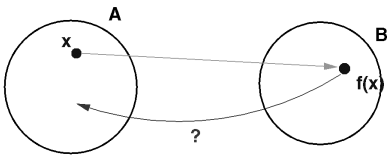
- Kryptographie: Entwurf von (sicheren) Systemen
- Kryptoanalyse: Brechen von Systemen
- Überbegriff für beides: Kryptologie

Klassifikation von kryptographischen Funktionen und Systemen

- Unkeyed
  - keine geheimen Schlüssel
  - one-way functions, hash functions
- Secret-Key
  - 2 oder mehrere „Einheiten“ (entities) verwenden die gleichen, geheimen Schlüssel
  - symmetrische Kryptographie
- Public-Key
  - keine gemeinsamen geheimen Schlüssel
  - asymmetrisch, Public-Key Kryptographie
  - digitale Signaturen

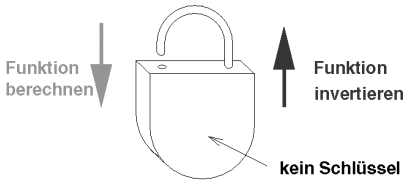
one-way function

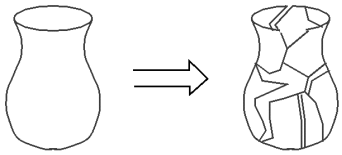
- Einwegfunktion
  - ist eine effizient berechenbare Funktion f von einer Menge *A* auf eine Menge *B*, *f: A→B*, so dass es „berechenmässig“ zu schwierig ist, für einen gegebenen Wert $y \in f(A)$ ein $x \in A$ zu finden mit $f(x) = y$
  - d.h.: *f* ist einfach zu berechnen, aber in der Praxis zu schwierig zu invertieren



one-way function

- mechanisches Analogon: Vorhängeschloss ohne Schlüssel



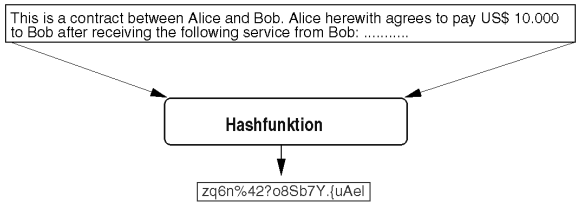


hash-function

- hash function
  - eine hash function ist eine effizient berechenbare Funktion *h* von einer Menge *A* auf eine Menge *B*, *h*: *A→B*, wobei |*B*| << |*A*|
  - eine Hashfunktion *h* heisst kollisionsfrei, wenn es berechenmässig zu schwierig ist, zwei verschiedene Werte *x* und *y* zu finden mit *h(x) = h(y)*
  - d.h.: eine Hashfunktion ist einfach zu berechnen, aber es ist zu schwierig, zwei Werte zu finden, die auf den gleichen Wert hashen

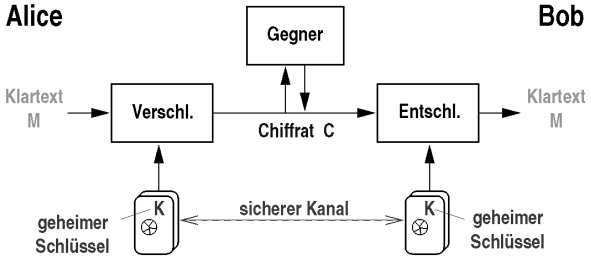
hash-function

- Kryptographische Hashfunktion



- Kollisionsfreiheit: Es ist berechenmässig zu schwierig, zwei Werte zu finden, die auf den gleichen Wert hashen

Symmetrisches Verschlüsselungssystem

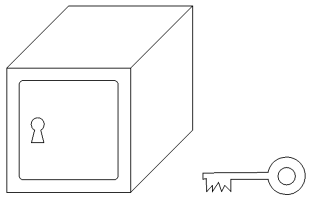


Symmetrisches Verschlüsselungssystem

- Sender: der Klartext M wird abhängig vom geheimen Schlüssel k zum Chiffrat C transformiert
- Übertragung erfolgt über einen „unsicheren“ Kanal (d.h. kann vom Gegner abgehört werden)
- Empfänger: nutzt den gleichen Schlüssel k um aus dem Chiffrat C wieder den Klartext M herzustellen
- beide Seiten (Sender und Empfänger) nutzen den gleichen Schlüssel k
- Hauptproblem: der Schlüssel k muss sicher übertragen werden und darf dem Gegner nicht bekannt sein
- Stichwort: Schlüsselmanagement

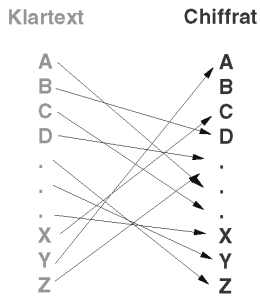
Symmetrisches Verschlüsselungssystem

- mechanisches Analogon:
  - Tresor mit einem Schlüssel



Symmetrisches Verschlüsselungssystem

- triviales Beispiel:
  - Monoalpabetische Substitution
  - trotz Schlüsselvielfalt einfach zu brechen durch statistische Häufigkeitsverteilung



Anzahl mögliche Schlüssel: $26! = 403'291'461'126'605'635'584'000'000$

Diffie-Hellman Protokoll (1976)

- Schlüsselverteilungsalgorithmus
  - zwei Kommunikationspartner wählen je einen geheimen Schlüssel
  - mit einer Einwegfunktion wird ein Wert hergeleitet (der sogenannte public key)
  - der public key wird übertragen über eine unsichere Datenleitung (die Übertragung muss authentisch sein)
  - beide können nun aus dem eigenen geheimen Schlüssel und dem public key des Partners einen gemeinsamen Schlüssel erstellen
  - dieser Schlüssel kann dann in einem symmetrischen Verschlüsselungssystem verwendet werden

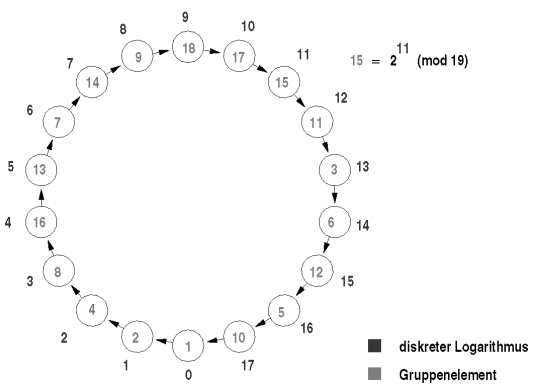
Diffie-Hellman key agreement protocol

- Sei p eine grosse Primzahl und g ein "Generator" von Z_p^* allgemein bekannt

Alice	insecure channel	Bob
choose x_A at random from $\{0,\ldots,p-2\}$		choose x_B at random from $\{0,\ldots,p-2\}$
$y_A \equiv g^{x_A} \pmod p$		$y_B \equiv g^{x_B} \pmod p$
	$y_A \rightarrow$	
	$\leftarrow y_B$	
$k_{AB} \equiv y_B{}^{x_A} \pmod p$		$k_{BA} \equiv y_A{}^{x_B} \pmod p$

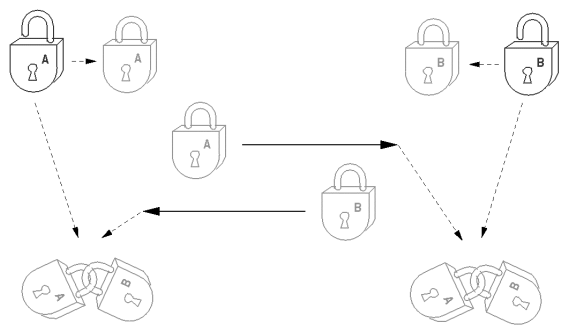
Common secret key: $k_{AB} \equiv y_B{}^{x_A} \equiv (g^{x_B})^{x_A} \equiv g^{x_A x_B} \equiv k_{BA} \pmod p$.

Diffie-Hellman



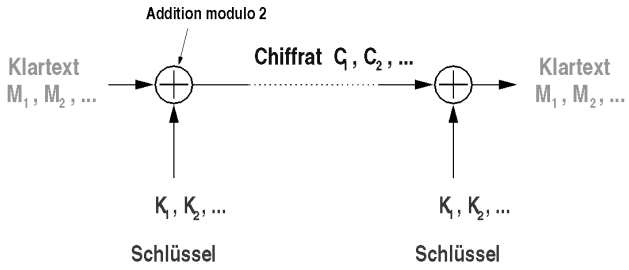
Diffie-Hellman

- mechanisches Analogon



Symmetrisches Verschlüsselungssystem

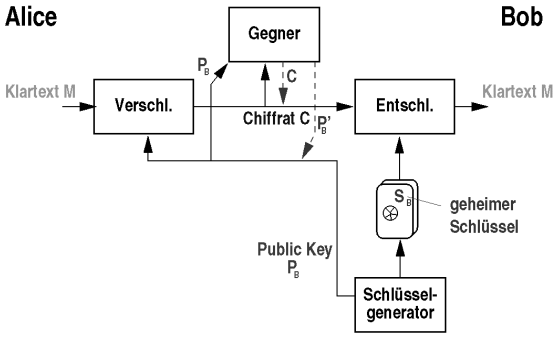
- One-Time Pad



Symmetrisches Verschlüsselungssystem

- One-Time Pad
  - stream-cipher
  - der Schlüsselstrom ist echt zufällig (nicht pseudo zufällig)
  - wird nur einmal verwendet
  - man kann beweisen, dass der one-time pad unbrechbar ist, selbst wenn der Gegner unendliche Computerressourcen besitzt
  - Hauptproblem bleibt das Schlüsselmanagement

Public-Key Kryptosystem

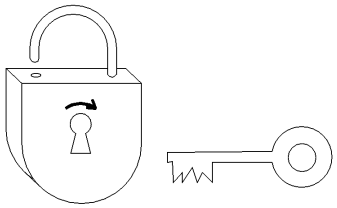


Public-Key Kryptosystem

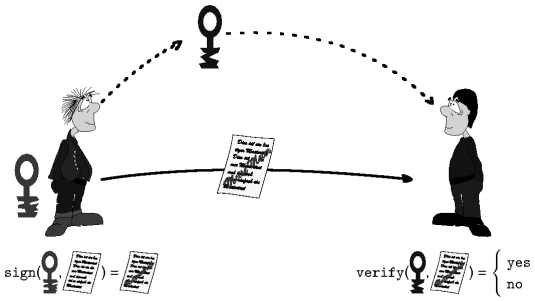
- Sender: verwendet den public key, um aus einem Klartext das Chiffrat zu erzeugen
- Übertragung des Chiffrats erfolgt über einen unsicheren Kanal
- Empfänger: verwendet den geheimen Schlüssel, um für das Chiffrat den entsprechenden Klartext zu erzeugen
- es gibt also 2 verschiedene Schlüssel
- der public key ist nicht geheim (Gegner darf ihn kennen)
- wichtig: Schlüsselgenerierung des geheimen Schlüssels und dem entsprechenden public key

Public-Key Kryptosystem

- mechanisches Analogon:
  - Vorhängeschloss, das jeder schliessen kann
  - aber nur mit einem bestimmten Schlüssel geöffnet werden kann

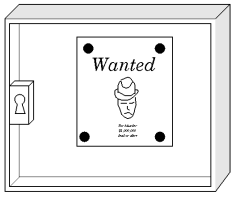


Digitale Signaturen

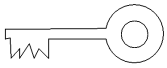


Digitale Signaturen

- Schlüsselgenerierungsverfahren (für geheimen Schlüssel und entsprechendem public key)
- Algorithmus zur Signatur-Generierung (unter Verwendung des geheimen Schlüssels)
- Algorithmus zur Signatur-Verifikation (unter Verwendung des public key)

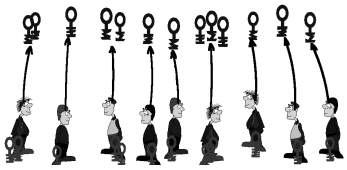


- **mechanisches Analogon:**
  - Schaukasten, zu dem nur einer einen Schlüssel hat



Public Key als digitale Repräsentanten

- jede Entität (Bsp: Person) generiert einen geheimen Schlüssel und den dazugehörigen public key, der als digitaler Repräsentant der Entität dient
- digitale Aktivitäten (Identifikation, Unterschrift unter digitalen Verträge, etc.) können an den public key gebunden werden



- notwendige Voraussetzung: Public Key Infrastruktur (PKI)

Public Key Zertifikate

- eine Zertifizierungsinstanz X bestätigt die Bindung zwischen einem public key P und einer Entität B
  - indem X den public key P signiert
- Grundidee: jeder, der
  (a) eine authentische Kopie des public key der Zertifizierungsinstanz X besitzt und
  (b) X vertraut (!)
  kann die Authentizität des public key P von B verifizieren

Kerberos

- **ermöglicht Benutzern und Servern in verteilten Systemen, sich einseitig oder gegenseitig zu authentisieren**
  - Authentifikationsserver (AS), mit dem jeder Benutzer einen gemeinsamen geheimen Schlüssel vereinbart
  - Ticket Granting Server(TGS) - der repliziert werden kann
  - der Benutzer wird authentifiziert durch den AS und der TGS erhält einen einen temporären geheimen Schlüssel zur Sicherung der Verbindung zum Benutzer

PGP - Pretty Good Privacy

- auf dem Internet weit verbreitet, frei erhältlich
- verwendet zur Authentisierung und Verschlüsselung von elektronischer Post
- jeder kann prinzipiell die Authentizität von öffentlichen Schlüsseln bescheinigen (Zertifikat ausstellen)
- wenn ein Benutzer einen Schlüssel authentisch beziehen will, entscheidet er selbst, welchen Entitäten er vertrauen will (Konzept des „web of trust“)
- Phil Zimmermann (Autor von PGP) ist von den USA angeklagt worden wegen Verletzung der Exportbestimmungen (inzwischen freigesprochen)

Public Key Infrastruktur (PKI)

- **PKI ist ein allgemeiner Begriff für**
  - die Ausgabe von Zertifikaten
  - den Rückruf von Public Keys und Zertifikaten
  - das Speichern und Abfragen von Zertifikaten (Datenbankaspekte)
  - gezieltes Sammeln von Evidenz für die Verifikation einer Aussage
  - Schlüsse ziehen aus digitaler Evidenz
  - ...

Politische Aspekte der Kryptographie

- nationale Sicherheit und Verbrechensbekämpfung vs. Datenschutz
- internationale Abhörpraxis
- Information Warfare und Wirtschaftsspionage
- US Export Restriktionen
- Gesetzliche Verankerung digitaler Signaturen

Schlussbemerkungen

- Informationssicherheit ist kritischer Faktor in der Entwicklung der Informationstechnologie
- Vertrauen ist fundamentale Ressource
- Datenschutz wird zu einem zentralen Thema der Gesellschaft
- staatliche Kontrolle der Kryptographie ist mittelfristig nicht haltbar
- Public Key Infrastruktur als Teil der globalen Informationsinfrastruktur